PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-168006
(43)Date of publication of application : 24.06.1997

(51)Int.Cl. H04L 9/16
G09C 1/00
H04H 1/00
H04J 3/00
H04L 9/36
H04N 7/167

(21)Application number : 07-326810
(22)Date of filing : 15.12.1995

(71)Applicant : HITACHI LTD
(72)Inventor : KURIHARA HIROSHI

(54) COMMUNICATION EQUIPMENT AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To surely synchronize switching of a scramble key with switching of scramble key information on a data stream by using a scramble key so as to scramble application data.
SOLUTION: A time division frame controller 13 acquires a scramble key corresponding to a version numberattribute identification information of the scramble key and a time division frame ID of object application data for scrambling from a scramble key table 15 based on the time division frame ID and the version number of ECM data received from a time division frame monitor circuit 12. Then an application data ciphering processing circuit 14 scrambles a time division frame of desired application data by using the received scramble key and writes the attribute identification information to an area of the time division frame of the application data and provides an output of the result as a ciphered data stream.

<hr size=2 width="100%" align=center>

CLAIMS

[Claim(s)]
[Claim 1]A communication apparatus comprising:
A multiplexing means outputted as one unenciphered data stream of a gestalt which carried out time multiplexing of at least one or more sending signalsand gave a time division frame of program-related-information data to a time division frame of this multiplexing sending signal.
A detection means to detect information about a scramble key which receives this unenciphered data streamsupervises each time division frame of this unenciphered data streamand is contained in this time division frame.
A scrambler means scrambled to a time division frame of a request of said sending signal using a scramble key according to information detected by this detection means.

[Claim 2]The communication apparatus according to claim 1wherein said sending signals are application data of any one or those combination of an audiovideoand data and said program-related-information data is the ECM data included information on a scramble key.
[Claim 3]The communication apparatus comprising according to claim 2:
A version number a time division frame of said ECM data indicates an updating change order of a scramble key to be.
An information indicator in which it is shown whether transmitted data of a time division frame of this ECM data are effective.
Including time division frame IDsaid scrambler meansA time division frame monitor means which supervises ID of each time division frame in response to an unenciphered data stream outputted from said multiplexing meansdetects a time division frame of said ECM data from this time division frame IDand takes out said version number and said information indicator.
A scramble key management tool which makes information about said version number and a scramble key correspondand manages itAn application-data encryption processing means scrambled to a time division frame of desired application dataSaid information indicator taken out by said time division frame monitor means and said version number are receivedA change of a scramble key is detected with a continuous change of this version number when this information indicator is effectiveBased on management information of said scramble key management toolit has the scramble key information corresponding to this version numberA time sharing frame control means to control said application-data encryption processing means to apply scramble to a time division frame of desired application data.

[Claim 4]The communication apparatus comprising according to claim 2:
Attribute identification information of a scramble key for which a time division frame

of said application data is needed at the time of employment.
Including time division frame IDsaid scrambler meansA time division frame monitor means which supervises ID of each time division frame in response to an unenciphered data stream outputted from said multiplexing meansdetects a time division frame of application data from this time division frame IDand takes out attribute identification information of said scramble key.
A scramble key management tool which manages information on a scramble key.
An application-data encryption processing means scrambled to a time division frame of a request of application dataAttribute identification information of this scramble key taken out by said time division frame monitor means is receivedA change of a scramble key is detected with change of attribute identification information of this scramble keyA time sharing frame control means to control said application-data encryption processing means to change a scramble key based on scramble key information on said scramble key management tooland to apply scramble to a time division frame of desired application data.

[Claim 5]A multiplexing means outputted as one unenciphered data stream of a gestalt which attached a time division frame of ECM data which carried out time multiplexing of at least one or more application dataand included information on a scramble key in a time division frame of these multiplexing application dataReceive this unenciphered data stream and each time division frame of this unenciphered data stream is supervisedA change of a scramble key is detected from information included in a time division frame of ECM dataA scrambler means scrambled to a time division frame of a request of said application data using a scramble key corresponding to detected this informationHave an external input interfacechange scramble key information based on information inputted from this external input interfaceand ECM data is createdHave a key switchover control means to send out to said multiplexing meansand said key switchover control meansHave a scramble key generating meansan ECM time division frame ID-scramble key management toolan ECM schedule management meansa timerand an ECM preparing meansit makes only a required number generate a scramble key generating meansand a scramble key an ECM schedule management meansHave an external input interface and time division frame ID of application data and ECM data and a renewal change interval of a scramble key are inputted from this external input interfaceMatchmanage time division frame ID of said inputted application data and said ECM dataand an ECM time division frame ID-scramble key management toolWhat attached a version number and attribute identification information of a scramble key which express an updating change order with each scramble key generated in said scramble key generating meansWhile matching and carrying out registration management to time division frame ID of ECM data which received from said ECM schedule management meansand time division frame ID of application dataPass this management information to a scramble key

management tool of said scrambler meansand a timerManage a renewal interval inputted from an external input interface of said ECM schedule management meansand an ECM preparing means creates ECM data in response to information which is carrying out registration management by said ECM time division frame ID-scramble key management toolAccording to renewal switching timing of a scramble key from said timerchange information on said scramble keysend out to said multiplexing means and said scrambler meansA time division frame monitor meansa scramble key management tooland an application-data encryption processing meansHave a time sharing frame control means and said time division frame monitor means supervises ID of each time division frame in response to an unenciphered data stream outputted from said multiplexing meansDetect a time division frame of ECM data from this time division frame IDtake out said version number and said information indicatorand said scramble key management toolManage information about a scramble key which received from said ECM time division frame ID-scramble key management tooland said time sharing frame control meansReceive this information indicator taken out by said time division frame monitor meansand this version numberand a change of a scramble key is detected with a continuous change of this version number when this information indicator is effectiveSaid application-data encryption processing means is controlled to apply scramble to a time division frame of desired application data with scramble key information corresponding to this version number based on management information of said scramble key management toolWhile said application-data encryption processing means applies scramble to a time division frame of desired application data with scramble key information received from said time sharing frame control meansA communication apparatus writing attribute identification information of this scramble key in arbitrary fields of a time division frame of these application data.

[Claim 6]Have the following and said key switchover control means A scramble key generating means and an ECM time division frame ID-scramble key management toolHave an ECM schedule management means and an ECM preparing meansand said scramble key generating meansGenerate only a required number and a scramble key said ECM schedule management meansHave an external input interface and time division frame ID of application data and ECM data is inputted from this external input interfaceMatchmanage time division frame ID of said inputted application data and said ECM dataand said ECM time division frame ID-scramble key management toolA scramble key generated in said scramble key generating means is receivedWhile making it correspond to time division frame ID of ECM data which received from an ECM schedule management meansand time division frame ID of application data and carrying out registration managementPass this management information to a scramble key management tool of said scrambler meansand an ECM preparing means creates ECM data in response to information which is carrying out registration management by said ECM time division frame ID-scramble key management toolAccording to

renewal switching timing of a scramble key from said timerchange information on said scramble keysend out to a multiplexing means and said scrambler meansA time division frame monitor meansa scramble key management tooland an application-data encryption processing meansHave a time sharing frame control means and said time division frame monitor means supervises ID of each time division frame in response to an unenciphered data stream outputted from said multiplexing meansDetect a time division frame of application data from this time division frame IDtake out attribute identification information of said scramble keyand said scramble key management toolManage information on a scramble key which received from said time division frame ID-scramble key management tooland said time sharing frame control meansReceive attribute identification information of this scramble key taken out by said time division frame monitor meansdetect a change of a scramble key with change of attribute identification information of this scramble keyand a scramble key is changed based on scramble key information on said scramble key management toolSaid application-data enciphering processing part is controlled to apply scramble to a time division frame of desired application dataA communication apparatuswherein said application-data encoding means gives scramble using a scramble key corresponding to information about a scramble key which received from said time sharing frame control means.

A multiplexing means outputted as one unenciphered data stream of a gestalt which attached a time division frame of ECM data which carried out time multiplexing of at least one or more application dataand included information on a scramble key in a time division frame of these multiplexing application data.

While managing an updating change interval of a scramble key which had an external input interface and was inputted from this external input interface for every time division frame of desired application dataA timer with an attribute identification information option with a function added to a time division frame of predetermined application data of an unenciphered data stream which changed attribute identification information of a scramble key based on this updating change intervaland was outputted from said multiplexing means.

This unenciphered data stream outputted from said timer with an attribute identification information option is receivedSupervise each time division frame of this unenciphered data streamand a change of a scramble key is detected from information included in a time division frame of application dataA scrambler means scrambled to a time division frame of desired application data using a scramble key corresponding to detected this information.

A key switchover control means to have an external input interfaceto change scramble key information based on information inputted from this external input interfaceto create ECM dataand to send out to said multiplexing means.

[Claim 7]It has a scrambler means for key switchover control by which it had in one a

function which a key switchover control means in the communication apparatus according to claim 5 hasand a function which a scrambler means hasA communication apparatus performing an input of information on a scramble keymanagementcreation of ECM dataetc. within said scrambler means for key switchover control.
[Claim 8]A function which a key switchover control means in the communication apparatus according to claim 6 hasand a function which a scrambler means hasIt has a scrambler means for key switchover control by which it had in one a function which a timer with an attribution information option hasA communication apparatus performing addition of an input of information on a scramble keymanagementcreation of ECM datamanagement of an updating change interval of a scramble keyand attribute identification information of a scramble key to a time division frame of desired application dataetc. within said scrambler means for key switchover control.
[Claim 9]A communication apparatus adding a function which a scrambler means has to an original function of a multiplexing means as a function of a multiplexing means in the communication apparatus according to claim 5and performing detection of information about surveillance of a time division frameand a scramble keyscrambleetc. within said multiplexing means.
[Claim 10]A function which a timer with an attribution information option has in the communication apparatus according to claim 6A function which a scrambler means has is added to an original function of a multiplexing means as a function of a multiplexing meansA communication apparatus performing detection of information about management of an updating change interval of a scramble keyaddition of attribute identification information of a scramble key to a time division frame of desired application datasurveillance of a time division frameand a scramble keyscrambleetc. within said multiplexing means.
[Claim 11]A communication apparatus doubling a function which a key switchover control means hasand a function which a scrambler means has in the communication apparatus according to claim 5adding to an original function of a multiplexing means as a function of a multiplexing meansand performing key switchover controlscrambleetc. within said multiplexing means.
[Claim 12]A function which a key switchover control means has in the communication apparatus according to claim 6and a function which a scrambler means hasA communication apparatus doubling a function which a timer with an attribute identification information option hasadding to an original function of a multiplexing means as a function of a multiplexing meansand performing addition of key switchover control and attribute identification information of a scramble key to desired application datascrambleetc. within said multiplexing means.
[Claim 13]In the communication apparatus according to claim 6a function which a timer with an attribute identification information option hasA communication apparatus adding to an original function of a multiplexing means as a function of a multiplexing meansand performing addition of management of an updating change

interval of a scramble keyand attribute identification information of a scramble key to a time division frame of desired application dataetc. within a multiplexing means.
[Claim 14]It is a correspondence procedure transmitted to a receiving side device as one data stream which multiplexed at least one or more sending signals to time sharingand was divided by a time division frameCarry out time multiplexing of at least one or more sending signalsand it outputs as one unenciphered data stream of a gestalt which gave a time division frame of program-related-information data to a time division frame of this multiplexing sending signalReceive this unenciphered data stream and each time division frame of this unenciphered data stream is supervisedA correspondence procedure detecting information about a scramble key contained in this time division frameand applying scramble to a time division frame of a request of said sending signal using a scramble key according to detected information.
[Claim 15]The correspondence procedure according to claim 14wherein said sending signals are application data of any one or those combination of an audiovideoand data and said program-related-information data is the ECM data included information on a scramble key.
[Claim 16]A version number a time division frame of said ECM data indicates an updating change order of a scramble key to beAn information indicator in which it is shown whether transmitted data of a time division frame of this ECM data are effectiveID of each time division frame of an unenciphered data stream by which time multiplexing was carried out is supervised including time division frame IDDetect a time division frame of ECM data from this time division frame IDand said version number and said information indicator are taken outA change of a scramble key is detected with a continuous change of this version number when this information indicator is effectiveBased on management information of a scramble key management table which has managed information on a scramble keyThe correspondence procedure according to claim 15 applying scramble to a time division frame of said desired application data with scramble key information corresponding to this version number.
[Claim 17]The correspondence procedure according to claim 15 changing a scramble key based on key information of a scramble key management table characterized by comprising the followingand applying scramble to a time division frame of desired application data.
Attribute identification information of a scramble key for which a time division frame of said application data is needed at the time of employment.
ID of each time division frame of an unenciphered data stream outputted by carrying out time multiplexing is supervised including time division frame IDA time division frame of application data is detected from this time division frame IDattribute identification information of said scramble key is taken outa change of a scramble key is detected with change of attribute identification information of this scramble keyand it is the information on a scramble key.

[Claim 18]It is a correspondence procedure transmitted to a receiving side device as one data stream which carried out time multiplexing of at least one or more application dataand was divided by a time division frameA multiplexing step outputted as one unenciphered data stream of a gestalt which attached a time division frame of ECM data which carried out time multiplexing of at least one or more application dataand included information on a scramble key in a time division frame of these multiplexing application dataReceive this unenciphered data stream and each time division frame of this unenciphered data stream is supervisedA change of a scramble key is detected from information included in a time division frame of ECM dataA scramble step scrambled to a time division frame of a request of application data using a scramble key corresponding to detected this informationBased on information set up beforehandchange scramble key informationand ECM data is createdConsist of a key switchover control step sent out to said multiplexing meansand registration management of attribute identification information and the version number is attached and carried out to each scramble key which generated only a required number and was made to generate a scramble key in said key switchover control stepRegistration management of time division frame ID of application data and ECM data set up beforehand is matched and carried outWhile passing this registration management information to a scramble key management table of a scramble stepECM data is created based on said registration management informationInformation on said scramble key is changed according to a renewal interval of a scramble key set up beforehandIn [perform processing which passes said ECM data to said multiplexing device stepand] said scrambler stepEach time division frame is supervised in response to an unenciphered data stream outputted from said multiplexing stepDetect a time division frame of ECM data from this time division frame IDand said version number and said information indicator are taken outA change of a scramble key is detected with a continuous change of this version number when this information indicator is effectiveBased on management information of a scramble key management table which made a version number and scramble key information correspondand has managed themscramble is applied to a time division frame of desired application data with scramble key information corresponding to this version numberA correspondence procedure performing processing which writes attribute identification information of this scramble key in arbitrary fields of a time division frame of these application data.

[Claim 19]A correspondence procedure transmitted to a receiving side device as one data stream which carried out time multiplexing of at least one or more application dataand was divided by a time division framecomprising:

A multiplexing step outputted as one unenciphered data stream of a gestalt which attached a time division frame of ECM data which carried out time multiplexing of at least one or more application dataand included information on a scramble key in a

time division frame of these multiplexing application data.
While managing an updating change interval of a scramble key set up beforehand for every time division frame of desired application dataA timer step with an attribute identification information option with a function which changes attribute identification information of a key based on this updating change intervaland adds attribute identification information of a key to a time division frame of predetermined application data of said unenciphered data stream.
This unenciphered data stream outputted from this timer step with an attribute identification information option is receivedSupervise each time division frame of this unenciphered data streamand change of a scramble key is detected from information included in a time division frame of application dataA scramble step scrambled to a time division frame of a request of said application data using a scramble key corresponding to detected this information.
Based on information set up beforehandchange scramble key informationand ECM data is createdIn [consist of a key switchover control step sent out to said multiplexing meansand] said key switchover control stepRegistration management of time division frame ID of application data and ECM data beforehand set to a scramble key which generated only a required number and was made to generate a scramble key is matched and carried outWhile passing this information that is carrying out registration management to a scramble key management table of a scrambler stepProcessing which creates ECM data based on this registration management informationchanges information on said scramble key according to a renewal change interval of a SUKURANMBURU key set up beforehandand passes said ECM data to said multiplexing device step is performedIn a scrambler stepID of each time division frame is supervised in response to an unenciphered data stream outputted from a timer step with an attribute identification information optionA time division frame of application data is detected from this time division frame IDattribute identification information of said scramble key is taken outa change of a scramble key is detected with change of attribute identification information of this scramble keyand it is the information on a scramble key.

[Claim 20]A communications system which has one or more transmitting side devices and one or more receiving side devicescomprising:
A multiplexing means outputted as one unenciphered data stream of a gestalt which a transmitting side device carried out time multiplexing of at least one or more sending signalsand gave a time division frame of program-related-information data to a time division frame of this multiplexing sending signal.
A means to detect information about a scramble key which receives this unenciphered data streamsupervises each time division frame of this unenciphered data streamand is contained in this time division frame.
Scramble is applied to a time division frame of a request of said sending signal using a

scramble key according to information detected by this detection meansA descrambler means for it to have a scrambler means to output as an enciphered data streamand for a receiving side device to receive an enciphered data stream sent from said transmitting side deviceand to descramble using a descrambling key corresponding to said scramble key.
A demultiplexing means to receive a descrambled this data stream and to dissociate for every sending signal.
A displaying means which displays a separated this signal.

[Claim 21]To a time division frame of a multiplexing sending signal multiplexed to time sharingat least one or more sending signals. It is a correspondence procedure which applies to which and transmits scramble to a time division frame of a sending signal of a request on one unenciphered data stream of a gestalt which a time division frame follows which attached a time division frame of program-related-information dataA scramble key is changed corresponding to change of information about a scramble key contained in the 1st time division frame in said continuous time division frameA correspondence procedure characterized by giving scramble using said scramble key to the 2nd time division frame that continues after this 1st time division frame.
[Claim 22]The correspondence procedure according to claim 21wherein said sending signals are application data of any one or those combination of an audiovideoand data and said program-related-information data is the ECM data included information on a scramble key.
[Claim 23]It is a time division frame of application data corresponding to a time division frame of said ECM data in said 2nd time division frame corresponding to a time division frame of ECM data in said 1st time division frameA version number a time division frame of said ECM data indicates an updating change order of a scramble key to beAs change of information about said scramble key including an information indicator in which it is shown whether transmitted data of a time division frame of this ECM data are effectiveThe correspondence procedure according to claim 22 using a continuous change of said version number when said information indicator is effective.
[Claim 24]Said 1st time division frame A time division frame of application dataThe 2nd time division frame is a time division frame of application data matched with a time division frame of these application dataand a time division frame of these application dataA time division frame of said application dataThe correspondence procedure according to claim 22 using change of attribute identification information of said scramble key contained in a time division frame of said application data as change of information about said scramble key including attribute identification information of a scramble key.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention about the system which requires privacy among the broadcasting systems or communications systems which transmit a multiplexing sending signal to a receiving terminalIn the image distribution system according to a personal-computer-communications system or a personal computer especiallya CATV systema terrestrial broadcasting systema satellite broadcasting systema satellite communication systemetc.It is related with the communication apparatus and correspondence procedure which can synchronize certainly the transmission switching sexagenary cycle of the time division frame included the change timing of a scramble key and the information on a scramble key which are applied to application data for secrecy-izing.
[0002]
[Description of the Prior Art]The change of the former and a scramble keyThe following is known as the technique of changing the entitlement control message data (Entitlement Control Message data: carry out abbreviated to ECM data below) which include the information about a scramble key in connection with it.
[0003]Equipping a multiplexing means with the input port only for ECM data firstECM data makes the priority of multiplexing to a time division frame higher than application data inputted from other input portssuch as video and an audio. And the data inputted from each input port without changing a transmission rateMake it the processing time within a multiplexing means until Time Division Multiplexing is carried out and it is outputted from a multiplexing means become fixedor set up the maximum of required processing time within a multiplexing meansand the maximum processing time is made into fixed timeAs a scramble key is delivered to a scramblerit changes to the scramble key specified for every fixed processing time of the in the scrambler and scramble is appliedthe change of a scramble key and the change of ECM data are performed.
[0004]
[Problem(s) to be Solved by the Invention]Thussince the timing which multiplexes ECM data to a data stream is decided by a multiplexing means and change timing of a scramble key is performed with a fixed time interval within a scramblerWhen disorder produced that it was also temporarywithout completing processing by a certain cause to the fixed processing time set up within the multiplexing meansin spite of having updated the scramble keythe combination etc. of the application data inputted into a multiplexing meansThe ECM data included the information on an old scramble key may be transmitted as an effective thing. In such a casein a receiverit becomes impossible to solve the scramble concerning application data. Such a phenomenon is a neck systematically and there was a problem that service will be interrupted by a

receiver temporarily.
[0005]In the updating change technique of the conventional scramble keysince a multiplexing means and meanssuch as a scramblerwere not able to be respectively manufactured independently with independent specificationwhen giving privacy to the existing transmission line which did not need privacythey also had the fault that the multiplexing means of another specification was needed. High performance nature and stringent specification are required and such a multiplexing means becomes expensive also in price.
[0006]The purpose of this invention is to provide the communication apparatus and correspondence procedure which may synchronize certainly the change of a scramble keyand the change of the scramble key information on a data stream. It enables it to prepare a scrambler means and a multiplexing means for the transmitting station side equipment independentlyand addition of the privacy to the transmission line which did not need the existing privacy aims at realization of a system with easy high flexibility.
[0007]
[Means for Solving the Problem]In order to attain these purposesa communication apparatus of this inventionInformation about a scramble key on scramble scramble application data by making processing time within a multiplexing means regularity like a conventional exampleand a data stream is not synchronizedOn a data stream after multiplexingform a means to detect an updating change of scramble key informationand desired application data are scrambled using a scramble key corresponding to detected scramble key informationScramble and scramble key information which are applied to application data are synchronized.
[0008]A communication apparatus indicated to Claim 5 containing the above-mentioned scrambler means is provided with the following.
A version number contained in ECM data of a data stream after multiplexing as information for detecting a change of a scramble key (an updating change order of a scramble key is expressed).
A multiplexing means outputted as one unenciphered data stream of a gestalt which gave a time division frame of ECM data to what carried out time multiplexing of at least one or more application data using an information indicator (it is shown whether transmitted data of ECM data are effective).
Receive an unenciphered data stream outputted from a multiplexing meansand each time division frame is supervisedA scrambler means which detects information about a scramble key contained in a time division frameand is scrambled to a time division frame of a request of application data using a scramble key corresponding to detected information.
A key switchover control means to have an external input interfaceto change scramble key information based on information inputted from the outsideto create ECM dataand to send out to a multiplexing means.

[0009]A key switchover control means Among thesea scramble key generating means and an ECM time division frame ID-scramble key management toolHave an ECM schedule management meansa timerand an ECM preparing meansand a scramble key generating meansGenerate only a required number and a scramble key an ECM schedule management meansIt has an external input interfaceand time division frame ID of application data and ECM data is matched and managed among time division frame ID of application data inputted from the outsideand ECM dataand a renewal change interval of a scramble key. An ECM time division frame ID-scramble key management toolA scramble key generated in a scramble key generating means is receivedand while carrying out registration management of a version number which expresses an updating change order of a scramble key to eachand the thing which attached attribute identification informationthe management information is passed to a scramble key management tool of a scrambler means. Manage a timer and a renewal interval of a scramble key inputted from an external input interface of an ECM schedule management means an ECM preparing meansECM data is created in response to information which is carrying out registration management by an ECM time division frame ID-scramble key management toolinformation on a scramble key is changed according to renewal switching timing of a scramble key from a timerand it sends out to a multiplexing device.

[0010]A scrambler means A time division frame monitor means and a scramble key management toolIt has an application-data encryption processing means and a time sharing frame control meansA time division frame monitor means supervises each time division frame in response to an unenciphered data stream outputted from a multiplexing meansand takes out a version number and an information indicator which are contained in a time division frame of ECM data. A time sharing frame control meansWhile judging existence of a change of a scramble key from a continuous change of a version number when an information indicator is effectiveinformation on a scramble key corresponding to the version number is acquired from a scramble key management tooland an application-data encryption processing means is passed. While an application-data encryption processing means scrambles a time division frame of desired application data based on information about a scramble key which received from a time sharing frame control meansAttribute identification information of a scramble key is added to arbitrary fields of scrambled application data.

[0011]A communication apparatus indicated to Claim 6 is provided with the following. As information for detecting a change of a scramble keyattribute identification information of a scramble key contained in application data of a data stream after multiplexing is usedA multiplexing means outputted as one unenciphered data stream of a gestalt which gave a time division frame of ECM data to what carried out time multiplexing of at least one or more application data.

While managing an updating change interval of a scramble key which had an external input interface and was inputted from the outside for every time division frame of

desired application dataA timer with an attribute identification information option with a function added to a time division frame of predetermined application data in an unenciphered data stream which changed attribute identification information of a scramble key based on an updating change interval of a scramble keyand was outputted from a multiplexing device.
an unenciphered data stream outputted from a timer with an attribute identification information option is receivedA scrambler means which detects information about a scramble key contained in a time division frame in a data streamand is scrambled to a time division frame of a request of said application data using a scramble key corresponding to detected information.
A key switchover control means to have an external input interfaceto change scramble key information based on information inputted from the outsideto create ECM dataand to send out to a multiplexing means.

[0012]A key switchover control means Among thesea scramble key generating means and an ECM time division frame ID-scramble key management toolHave an ECM schedule management means and an ECM preparing meansand a scramble key generating meansonly a required number generates a scramble key -- an ECM schedule management means has an external input interfaceand matches and manages time division frame ID of application data inputted from the outsideand ECM data. An ECM time division frame ID-scramble key management toolWhile making it correspond with time division frame ID of ECM data and time division frame ID of application data which were received from an ECM schedule management means in response to a scramble key generated in a scramble key generating means and carrying out registration managementThe management information is passed to a scramble key management tool of a scrambler means. An ECM preparing means creates ECM data in response to information which is carrying out registration management by an ECM time division frame ID-scramble key management toolInformation on said scramble key is changed according to renewal switching timing of a scramble key from a timer with an attribute identification information option which manages a renewal change interval of a scramble keyand it sends out to a multiplexing device.
[0013]A scrambler means A time division frame monitor means and a scramble key management toolIt has an application-data encryption processing means and a time sharing frame control meansA time division frame monitor means supervises each time division frame in response to an unenciphered data stream outputted from a multiplexing meansand takes out attribute identification information of a scramble key contained in a time division frame of application data. A time sharing frame control means acquires information on a scramble key from a scramble key management tooland passes it to an application-data encryption processing means while it judges existence of a change of a scramble key from change of attribute identification

information of this scramble keyAn application-data encryption processing means scrambles a time division frame of desired application data based on information about a scramble key which received from a time sharing frame control means.
[0014]
[Embodiment of the Invention]About an embodiment of the inventiontwo or more working example is given and described below.
[0015]working example 1 -- the 1st working example that detects the change of a scramble key is first described from the version number contained in the time division frame of the ECM data on a multiplexing data streamand an information indicator. Hereas a multiplexing data streamthere are some which are described by MPEG-1 SYSTEMS (ISO/IEC 11172-1) and MPEG-2 SYSTEMS (ISO/IEC 13818-1)for example. It is equivalent to the session key called scramble keyfor example by the key arrangement in a charged scramble broadcast network. A time division frametime division frame IDa version numberand an information indicatorThe transport packet described by the MPEG-2 SYSTEMS (TSP:Transport Stream Packet)A packet identifier (PID:Packet Identifier)Version numberssuch as program specification information (PSI:Program Specific Information) (version number)It carries out considerable to current NeXT identifiers (current next identifier)such as PSIrespectivelyA version number is a value given in order of the updating change of a scramble keyand an information indicator is a value which shows whether the information included in the ECM data is effective or invalid.
[0016]Drawing 1 is a scrambler with the key change detection function in this invention. As for a time division frame supervisory circuit and 13in drawing 11 is [an application-data encryption processing circuit and 15] scramble key management tables a time sharing flame controller and 14 a scrambler and 12.
[0017]The input to a scrambler is the unenciphered data stream outputted by attaching the time division frame of the ECM data which multiplexed at least one application data to time sharing in the multiplexing deviceand included the information on a scramble key. The unenciphered data stream inputted into the scrambler is inputted into a time division frame supervisory circuit in order of the time division frame at the time of an input. In a time division frame supervisory circuitID of the time division frame which exists in the predetermined field of each time division frame of an unenciphered data stream is supervised. And the time division frame of ECM data is detected from time division frame IDan information indicator is acquired with the version number contained in the ECM dataand a time sharing flame controller is passed with time division frame ID of ECM data. A time sharing flame controller detects the scramble key having been updated and having changedwhen an information indicator is effective as compared with the last version number and a version number changes continuously the version number received from the time division frame supervisory circuit. The scramble key corresponding to the version number from a scramble key management table based on time division frame ID and

the version number of ECM data which received the time sharing flame controller from the time division frame supervisory circuitThe attribute identification information of a scramble key and time division frame ID of the object application data to scramble are acquiredand the information is passed to an application-data encryption processing circuit. An application-data encryption processing circuit applies scramble using the scramble key which received the information to the time division frame of the application data for which it receives and asksThe attribute identification information of a key is written in in the field of the time division frame of the application dataand it outputs as an enciphered data stream. As opposed to the time division frame of the application data which are not scrambledThe judgment which is not scrambled in a time sharing flame controller is carried out via a time division frame supervisory circuitand it carries out throughwithout applying scramble in an application-data encryption processing circuit.

[0018]The lineblock diagram of the main part of a transmitting side device including the scrambler of drawing 1 is shown in drawing 2. In drawing 21 a scrambler and 2 a key switching control device and 3 A multiplexing deviceA time division frame supervisory circuit and 13 12 A time sharing flame controllerAn application-data encryption processing circuit and 15 14 A scramble key management table16 -- as for an ECM time division frame ID **SUKU rumble lock management circuit and 20an ECM creation circuit and 18 are [a scramble key generation circuit and 22] unenciphered ECM control circuits an ECM schedule management circuit and 21 a timer and 19 an enciphering circuit and 17.

[0019]In the key switching control device of drawing 2an ECM schedule management circuitWhile matching with time division frame ID of the ECM data which had an external input interface and was inputted from the outsideand time division frame ID of application data and managingthe information An ECM creation circuitAn ECM time division frame ID-scramble key control circuit and an unenciphered ECM control circuit are passed. From the exteriorthe renewal interval of a key change is set up for every application data to scrambleand the renewal interval by which input setting was carried out here is made to correspond with time division frame ID of ECM dataand is passed to a timer. an unenciphered ECM control circuit has an external input interfacesets up ECM syntax freely from the exterioris matched with time division frame ID of the ECM data into which the ECM syntax inputted from the outside was inputted from the ECM schedule management circuitand manages it. On the other handin a scramble key generation circuitthe scramble key which made it generate in order of an updating changeand was made to generate the scramble key for several updating changes according to time division frame ID of ECM data beforehand is passed to an ECM time division frame ID-scramble key control circuit. An ECM time division frame ID-scramble key control circuitThe attribute identification information of the scramble key which is needed for the received scramble key by the scramble transmission system in the service to employ itself in order of the updating change of

a scramble key EvenOddEvenand Odd -- or it giving OddEvenOddEvenand by turnsandThe version number which expresses an updating change order of a scramble key with each scramble key in order of an updating change is assignedThese information is made to correspond with the group of time division frame ID of application data for every ID of the time division frame of the ECM data received from the ECM schedule management circuitand is managed. An ECM time division frame ID-scramble key control circuit is passed by forward [to which a scramble key becomes effective to application data about the information about these scramble keys managed for every ECM time division frame ID to the scramble key management table of a scrambler]. ECM data is created based on the information managed in the ECM time division frame ID-scramble key control circuit in the ECM creation circuitand it enciphers about the information on a scramble key in an enciphering circuitand sends out to a multiplexing device. The information about the scramble key of ECM data is changed according to the updating change interval of the scramble key managed with the timer.

[0020]In a multiplexing deviceas the data A1data A1'the data B1and the data C1 show by drawing 2Application datasuch as one or more audios and videoare multiplexed to time sharingand the ECM data sent from the key switching control device is attachedit outputs as one unenciphered data streamand a scrambler is passed.

[0021]Since it is as having explained operation of each block of a scrambler in drawing 1the composition of a time division frame and the example of composition of a multiplexing data stream are shown hereand explanation of a scrambler of operation is given.

[0022]Firstthe composition of the time division frame of ECM data is shown in drawing 10and the composition of the time division frame of application data is shown in drawing 11. As for time division frame ID and 31in drawing 10an information indicator and 33 are the information on a scramble key a version number and 32 30. The information on the scramble key of 33 added shading and shown with the slash is a portion to which encryption is given in the enciphering circuit of a key switching control device. On the other hand in drawing 11it is an information area of the application data for which time division frame ID stores 30the attribute identification information of a scramble key is stored 34and the data of videoan audioetc. is stored 35. The portion added shading and shown with the slash of 35 is a field which gives scramble in the application-data encryption processing circuit of a scrambler. Each one time division frame ID of every per application data and ECM data kind gives. In drawing 2one is assigned at a time at a time to the application data A1A1'B1and C1 at one ECM. As shown in drawing 10the time division frame of ECM data includes the version number which shows an updating change order of a scramble keythe information indicator in which it is shown whether the transmitted data of the time division frame of the ECM data are effective or invalidand the information on a scramble key. The time division frame of application data contains the attribute

identification information of the scramble key which is needed at the time of employmentas shown in drawing 11.
[0023]Multiplexing these time division frames in a multiplexing devicein response to the unenciphered data stream after multiplexinga scrambler applies scramble to the time division frame of desired application dataand outputs an enciphered data stream. The enciphered data stream which is an output from a scrambler at drawing 12 about the unenciphered data stream which is an input to a scrambler is shown in drawing 13. In [in drawing 12363738and 39 are the time division frames of ECM data and] drawing 13As for an information indicator and 3431 is [the time division frame of the application data A1 and 41] the time division frames of application-data A1' the attribute identification information of a scramble keyand 40 a version number and 32.
[0024]The unenciphered data stream shown in drawing 12 is inputted into a scrambler sequentially from a right-hand side time division frame. In a scramblerID of each time division frame is supervised in a time division frame supervisory circuitthe time division frame of ECM data is detected from IDand a version number and an information indicator are taken out. Herethe time division frame of 36 is detected first. It judges with the transmitted data of the time division frame of 36 being more invalid than the information indicator which received the time sharing flame controller from the time division frame supervisory circuitand the scramble key not having changed. Nexta time division frame supervisory circuit detects the time division frame of the ECM data of 37. Heresuppose that the version number of the effective ECM data detected last time was n-2. Since the time division frame of the ECM data of 37 has an effective information indicator and change of a version number is as continuous as n-2 to n-1a time sharing flame controllerThe information from which the scramble key changed carry out thing detection and concerning a scramble key and a key based on a scramble key management table to this version number is acquired.
[0025]The storing imaged figure of the scramble key information in a scramble key management table is shown in drawing 16. The scramble key management table made time division frame ID of the application data of the object to scramblea scramble keya version numberand the attribute identification information of the scramble key correspond for every time division frame ID of ECM dataand is managed. time sharing -- a flame controller -- ECM -- data -- a time division frame -- ID -- a version number -- n -one -- a basis -- a scramble key -- a management table -- from -- scramble -- applying -- an object -- application data -- A -- one -- A -- one -- ' -- ID. Scramble key Kn-1 and the attribute identification information Odd of a scramble key are acquiredand an application-data encryption processing circuit is passed. An application-data encryption processing circuit applies scramble using scramble key Kn-1 received to the time division frame of the application data A1 and A1'The attribute identification information Odd of a scramble key is written in the arbitrary fields of the time division frame of object application data.
[0026]In the enciphered data stream of drawing 1340 and A1' are carried out by

41and it adds shading to the application data A1 to which scramble was given with a slashand they are shown. 34 is the attribute identification information of the scramble key written in into the time division frame of application data in the application-data encryption processing circuit. Similarlya scramble key is changed to Kn also about the ECM time division frame 38the application data A1 and A1' are scrambledand the attribute identification information Even of a scramble key is written in the arbitrary fields of the time division frame of object application data. Henceforth detects the time division frame 39 of ECM similarlyand changes a scramble key. As a resultin the enciphered data stream shown in drawing 13The inside of the time division frame of the application data which make a head the time division frames 3738and 39 of ECM dataand follow itScramble is given using the information on the scramble key contained in the time division frames 3738and 39 of ECM data to the thing corresponding to the ECM data.

[0027]The 2nd working example is described to the secondary working example. In the 2nd working examplethe change of the scramble key given to the time division frame of the application data is detected from the attribute identification information of the scramble key contained in the time division frame of the application data of the request on a multiplexing data stream.

[0028]The lineblock diagram of the transmitting side equipment in the 2nd working example is shown in drawing 3. In drawing 3the point of difference with working example 1 shown in drawing 2 is at the point used as the timer 23 with an attribute identification information option which arranges the timer arranged in the key switching control device after a multiplexing deviceand has an attribute identification information option by drawing 2. A scrambler [in / on drawing 3 and / in 4 / working example 2]a key switching control device [in / in 5 / working example 2]A time division frame supervisory circuit [in / in 24 / working example 2]a time sharing flame controller [in / in 25 / working example 2]26 is an application-data encryption processing circuit in working example 2a scramble key management table [in / in 27 / working example 2]an ECM time division frame ID **SUKU rumble lock management circuit [in / in 28 / working example 2]and an ECM schedule management circuit [in / in 29 / working example 2]. Operation of each block is explained below. The other blocks attach the same numerals as drawing 2 in order to operate like working example 2.

[0029]In the key switching control device of drawing 3operation of an ECM schedule management circuitan unenciphered ECM control circuita scramble key generation circuitand an enciphering circuit is the same as that of working example 1. In an ECM time division frame ID-scramble key control circuitthe attribute identification information of a scramble key does not give in working example 2. The data passed to the lock management table of a scrambler is time division frame ID of ECM datatime division frame ID of the application data corresponding to itand the information on a scramble key. ECM data was created based on the information managed in the ECM

time division frame ID-scramble key control circuit in the ECM creation circuitand it has sent out to the multiplexing device. The information about the scramble key of ECM dataIt has changed according to the updating change interval of the scramble key managed for every time division frame of desired application data in a timer with an attribute identification information optionand the information on a scramble key has enciphered in the enciphering circuit.

[0030]In the 2nd working examplea multiplexing device carries out time multiplexing of the application datasuch as one or more audios and videoThe time division frame of the ECM data sent from the key switching control device is attachedit outputs as one unenciphered data streamand a timer with an attribute identification information option is passed.

[0031]The timer with an attribute identification information option has an external input interfacemakes ID of the time division frame of the application data which apply the updating change interval and its updating change interval of the scramble key inputted from the outside correspondand is managed. And the time division frame of application data is detected from time division frame ID of the unenciphered data stream received from the multiplexing devicebeing based on the updating change interval which was made to correspond with application-data ID and has been managed -- the attribute identification information of a scramble key -- EvenOddEvenand Odd -- or it changes to OddEvenOddand Even by turnsand writes in the arbitrary fields of application data.

[0032]Explanation of a scrambler of operation is given to drawing 14 and drawing 15 by showing the example of composition of a multiplexing data stream. This example describes only the group of the application data A1 and A1'. Drawing 14 shows the unenciphered data stream inputted into a scramblerandas for 42the time division frame of application-data A1' and 44 are the time division frames of application-data A1' the time division frame of the application data A1and 43. The unenciphered data stream of drawing 14 is inputted into a scrambler sequentially from a right-hand side time division frame. In a scramblerID of each time division frame is supervised in a time division frame supervisory circuitthe time division frame of application data is detected from IDand the attribute identification information of time division frame ID and a scramble key is taken out. In drawing 14the time division frame of the application data A1 of 42 is detected first. Heresuppose that the attribute identification information contained in the time division frame of the application data A1 detected last time was Even. The change of a scramble key is detected from the time sharing flame controller having changed from the attribute identification information Even of the time division frame of the group of the same application data that the attribute identification information of the scramble key of the time division frame of 42 detected last time to OddBased on time division frame ID of application dataa scramble key is acquired from a scramble key management table. The storing imaged figure of the scramble key information on the scramble key management table

in the 2nd working example is shown in drawing 17. A scramble key is managed with time division frame ID of ECM data for every group of time division frame ID of the application data of the object to which a scramble key management table and scramble are applied. A time sharing flame controller acquires Kn−1 which is the next scramble key of scramble key Kn−2 used last time from a scramble key management table based on time division frame ID of the application data A1and passes it to an application−data encryption processing circuit. An application−data encryption processing circuit applies scramble using scramble key Kn−1 received to the time division frame of the application data A1. Nextalthough a time division frame supervisory circuit detects the time division frame 43 of application−data A1'A1' is a group of the application data which apply the same scramble key as A1and since the attribute identification information of the scramble key has not changed with Oddsimilarly it gives scramble using scramble key Kn−1. After a time division frame supervisory circuit detects some time division frames of other application data similarlyThe time division frame 44 of application−data A1' is detectedit detects that the attribute identification information of a scramble key has changed to Even in a time sharing flame controllera scramble key is changed to Knand scramble is given. In the enciphered data stream of drawing 1545 and A1' are carried out by 46and it adds shading to the application data A1 to which scramble was given with a slashand they are shown. On the following data streamsa scramble key is similarly changed based on change of the attribute identification information of a scramble key. The same may be said of the time division frame of other application data.

[0033]Working example 3 drawing 4 is a lineblock diagram of the transmitting side device of the 3rd working example that serves as a scrambler for key switchover control having the function of the scrambler in the 1st working example of drawing 2and a key switching control device from a multiplexing device. In drawing 46 is a scrambler for key switchover control. Matching with the information inputted in this example from generating of a scramble key which the key switching control device was performing in the 1st working examplethe generated scramble keyand the outsidemanagementcreation of ECM dataetc.Detection of the information about the surveillance of a time division frame which the scrambler was performingand a scramble keyscramble processing based on the detected informationetc. are altogether performed in the scrambler for key switchover control. In order that each block in the scrambler for key switchover control and a multiplexing device may carry out the same operation as what was explained in drawing 2they attach the same numerals and omit explanation here.

[0034]Working example 4 drawing 5 is a lineblock diagram of the transmitting side device of the 4th working example that serves as a scrambler for key switchover control having the function of the timer with an attribute identification information option and scrambler in the 2nd working example of drawing 3and a key switching control device from a multiplexing device. In drawing 57 is a scrambler for key

switchover control with a timer with an attribute identification information option. Generating of a scramble key which the key switching control device was performing in the 2nd working example in this examplematching with the information inputted from the generated scramble key and the outside and managementcreation of ECM dataetc.Addition to the time division frame of the application data of the attribute identification information of the scramble key which the timer with an attribute identification information option was performingcontrol of the updating change interval of a scramble keyetc.In the scrambler for key switchover control with a timer with an attribute identification information optionall of detection of the information about the surveillance of a time division frame which the scrambler was performingand a scramble keythe scramble processing based on the detected informationetc. are performed. In order that each block in the scrambler for key switchover control with a timer with an attribute identification information option and a multiplexing device may carry out the same operation as what was explained in drawing 3they attach the same numerals and omit explanation here.

[0035]Working example 5 drawing 6 is a lineblock diagram of the multiplexing device added to the original function for which a multiplexing device has a function which the scrambler in the 1st working example of drawing 2 has as a function of a multiplexing deviceand the transmitting side device of the 5th working example that has a key switching control device. In drawing 68 is a multiplexing device with a scramble function. The time multiplexing of application data and ECM data etc. which the multiplexing device was performing in the 1st working example in this exampleIn a multiplexing device with a scramble functiondetection of the information about the surveillance of a time division frame which the scrambler was performingand a scramble keyscramble processing based on the detected informationetc. are performed. In order that each block in a multiplexing device with the scramble function of this example and a key switching control device may carry out the same operation as what was explained in drawing 2they attach the same numerals and omit explanation here.

[0036]Working example 6 drawing 7 is a lineblock diagram of the timer with an attribute identification information option in the 2nd working example of drawing 3the multiplexing device added to the original function for which a multiplexing device has a function which a scrambler has as a function of a multiplexing deviceand the transmitting side device in the 6th working example that has a key switching control device. In drawing 79 is a multiplexing device with a scramble function and a timer with an attribute identification information option. The time multiplexing of application data and ECM data etc. which the multiplexing device was performing in the 2nd working example in this exampleThe writing to the time division frame of the application data of the attribute identification information of the scramble key which the timer with an attribute identification information option was performingcontrol of the change interval of a scramble keyetc.In a multiplexing device with a scramble

function and a timer with an attribute identification information optionthe surveillance of a time division frame which the scrambler was performingdetection of a change of a scramble keyscrambleetc. are performed. In order that each block in a multiplexing device with the scramble function of this example and a timer with an attribute identification information option and a key switching control device may carry out the same operation as what was explained in drawing 3they attach the same numerals and omit explanation here.

[0037]Working example 7 drawing 8 is a lineblock diagram of the transmitting side device in the 7th working example that added the scrambler in the 1st working example of drawing 2and the function which a key switching control device has to the original function of the multiplexing device as a function of a multiplexing device. In drawing 810 is a multiplexing device with a key switchover control function and a scramble function. Generating of a scramble key which the key switching control device of the 1st working example was performing in this examplematching with the information inputted from the generated scramble key and the outside and managementcreation of ECM dataetc.In a multiplexing device with a key switchover control function and a scramble functionthe time multiplexing of application data and ECM data etc. which the multiplexing device was performingthe surveillance of a time division frame which the scrambler was performingdetection of a change of a scramble keyscrambleetc. are performed. In order that each block in a multiplexing device with the key switchover control function and scramble function of this example may carry out the same operation as what was explained in drawing 2it attaches the same numerals and omits explanation here.

[0038]Working example 8 drawing 9 is a lineblock diagram of the transmitting side device in the 8th working example that added the timer with an attribute adding function function in the 2nd working example shown in drawing 3the scramblerand the function that a key switching control device has to the original function of the multiplexing device as a function of a multiplexing device. In drawing 911 is a key switchover control functiona timer with an attribute identification information optionand a multiplexing device with a scramble function. Generating of a scramble key which was being performed with the key switching control device of the 2nd working example in this examplematching with the information inputted from the generated scramble key and the outside and managementcreation of ECM dataetc.The time multiplexing of application data and ECM data etc. which the multiplexing device was performingThe writing to the time division frame of the application data of the attribute identification information of the scramble key which the timer with an attribute identification information option was performingcontrol of the change interval of a scramble keyetc.In a key switchover control functiona timer with an attribute identification information optionand a multiplexing device with a scramble functionthe surveillance of a time division frame which the scrambler was performingdetection of a change of a scramble keyscrambleetc. are performed. In

order that each block in a multiplexing device with the key switchover control functionthe timer with an attribute identification information optionand scramble function of this example may carry out the same operation as what was explained in drawing 3it attaches the same numerals and omits explanation here.
[0039]Working example 9 drawing 19 is a lineblock diagram of the transmitting side device in the 9th working example that added the function which the timer with an attribute identification information option in the 2nd working example shown in drawing 3 has to the original function of the multiplexing device as a function of a multiplexing device. In drawing 1954 is a multiplexing device with a timer with an attribute identification information option. The management of the updating change interval of a scramble key which was being performed with the timer with an attribute identification information option of the 2nd working example in this exampleIn a multiplexing device with a timer with an attribute identification information optionaddition of the attribute identification information of the scramble key to the time division frame of desired application dataetc. are performed. In order that each block of the scrambler of this example and a key switching control device may carry out the same operation as what was explained in drawing 3it attaches the same numerals and omits explanation here.
[0040]Although not illustratedworking example for which the transmitting side device in working example 135and 7 described by drawing 2drawing 4drawing 6and drawing 8 does not need the attribute identification information of a scramble key by service to employ is also considered. In that caseattribute identification information is not given to the scramble key which received from the scramble key generation circuit in the time division frame ID-scramble key control circuit of a key switching control device. The information sent to the scramble key management table of a scrambler from a time division frame ID-scramble key control circuitThey are a group of time division frame ID of each ECM dataand time division frame ID of application data matched with itthe information on a scramble keyand a version number. The application-data encryption processing circuit of a scramblerIt does not have a function which writes the attribute identification information of a scramble key in the time division frame of application dataand the attribute identification information of the scramble key is not contained in the time division frame of the application data outputted from a scrambler.
[0041]The lineblock diagram 18 of the system by which this invention is applied is a lineblock diagram of the communications system which applies the communication apparatus of this invention. in drawing 18 -- 47 -- as for a receiving side device and 51the transmitting station side device and 49 are [a demultiplexing circuit and 53] TV monitors a descrambler and 52 a transmission line and 50 a broadcasting station and 48. The transmitting side device of 48 may be the composition shown in the 1st working example of this invention hereand although it has the multiplexing device 3the scrambler 1and the key switching control device 2it may be the composition shown in

other working example. The program created at the broadcasting station etc. consists of application datasuch as video and an audioWith a transmitting side devicein a multiplexing devicethese application data are multiplexed to time sharingthe time division frame of the ECM data created with the key switching control device is attachedand it outputs as one unenciphered data stream. A scrambler receives this unenciphered data streamdetects the information about the scramble key contained in the time division frame on a streamgives scramble using the scramble key corresponding to the detected informationand transmits an enciphered data stream. The transmission method at this time can consider the case where a cablea terrestrial wavea satelliteetc. are used. A receiving side device receives the transmitted enciphered streamand scramble is canceled using the descrambling key corresponding to the scramble key in the transmitting side in a descramblerIt views and listens to the program which separated application data multiplexed in the demultiplexing circuitsuch as video and an audiorespectivelydisplayed video and an audio with displayssuch as TV monitorand was created at the broadcasting station.
[0042]In each working example described beyond the effect of working exampleIt is made for a scrambler to detect on the data stream after multiplexing the change of scramble key informationWhen a scrambler changes a scramble key according to the scramble key information on the detected data streama synchronization is certainly establishable by the change of a scramble keyand the change of the scramble key information on the data stream after multiplexing. Thereforethe ECM data which included the information on an old scramble key in the scramble key having been updated and having changed is transmitted as an effective thing at presentor the thing so that it may become reverse is prevented. Thereforein a receiving side deviceit becomes possible to solve the scramble concerning application data certainly.
[0043]As a measure when viewing and listening becomes impossiblewithout confusing the synchronization with the information about a scramble key and the scramble key contained on a data stream in a transmitting side deviceand scramble solving in a receiver conventionallyThere was a case where searched a right descrambling key from the descrambling key information given by alternative pathwaywithout being based on the information on the scramble key on the transmitted multiplexing data streamand scramble was provided in the ********** function by the receiving side device. Since a synchronization is certainly establishable by the change of a scramble keyand the change of the scramble key information on a multiplexing data streamit becomes unnecessary to give such an excessive function to a receiving side device according to this invention.
[0044]In working example 1working example 2working example 3working example 4and working example 9In working example 1it is with a scrambler and a key switching control device about the function which is needed by secrecy-ization of data transmissionIn working example 2it is with a timer with an attribute identification information optionand a scrambler and a key switching control deviceand a

transmitting side device can be independently equipped with a multiplex processing section by constituting from a scrambler for key switchover control in working example 3 and 4. Thereforeaddition of the privacy to the existing communications system which did not need privacy becomes easyand a system with high flexibility can be constituted.

[0045]

[Effect of the Invention]According to the communication apparatus and correspondence procedure of this inventionregardless of the processing time in a multiplexing deviceIt is made for a scrambler to detect on the data stream after multiplexing change of scramble key informationWhen a scrambler performs scramble using the scramble key corresponding to the scramble key information on the detected data streama synchronization is certainly establishable by the change of a scramble keyand the change of the scramble key information on the data stream after multiplexing. Thereforein a receiving side deviceit becomes possible to solve the scramble concerning application data certainly.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure of the scrambler of this invention.

[Drawing 2]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 3]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 4]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 5]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 6]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 7]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 8]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 9]It is a figure of the transmitting station side device of one working example of this invention.

[Drawing 10]It is an example of information composition of the time division frame of ECM data.

[Drawing 11]It is an example of information composition of the time division frame of application data.

[Drawing 12]It is an example of composition of the unenciphered data stream inputted into the scrambler in the 1st working example.
[Drawing 13]It is an example of composition of the enciphered data stream outputted from the scrambler in the 1st working example.
[Drawing 14]It is an example of composition of the unenciphered data stream inputted into the scrambler in the 2nd working example.
[Drawing 15]It is an example of composition of the enciphered data stream outputted from the scrambler in the 2nd working example.
[Drawing 16]It is a storing imaged figure of the information about the scramble key and scramble key of a scramble key management table in the 1st working example.
[Drawing 17]It is a storing imaged figure of the information about the scramble key and scramble key of a scramble key management table in the 2nd working example.
[Drawing 18]It is a lineblock diagram of the whole communications system with which this invention is applied.
[Drawing 19]It is a figure of the transmitting station side device of one working example of this invention.
[Description of Notations]
1 [-- The scrambler in working example 2] -- A scrambler2 -- A key switching control device3 -- A multiplexing device4 5 -- The key switching control device in working example 26 -- The scrambler for key switchover control7 -- The scrambler for key switchover control with a timer with an attribute identification information option8 -- A multiplexing device with a scramble function9 -- A multiplexing device with a scramble function and a timer with an attribute identification information option10 -- A multiplexing device with a key switchover control function and a scramble function11 -- A key switchover control functiona timer with an attribute identification information optionand a multiplexing device with a scramble function12 -- A time division frame supervisory circuit13 -- Time sharing flame controller14 -- An application-data encryption processing circuit15 -- Scramble key management table16 [-- ECM time division frame ID **SUKU rumble lock management circuit] -- An enciphering circuit17 -- An ECM creation circuit18 -- A timer19 20 [-- A timer with an attribute identification information option24 / -- The time division frame supervisory circuit in working example 225 / -- The time sharing flame controller in working example 2] -- An ECM schedule management circuit21 -- A scramble key generation circuit22 -- an unenciphered ECM control circuit23 26 -- The application-data encryption processing circuit in working example 227 -- The scramble key management table in working example 228 -- The ECM time division frame ID **SUKU rumble lock management circuit in working example 229 -- The ECM schedule management circuit in working example 230 -- Time division frame ID31 -- A version number32 -- An information indicator33 -- Information on a scramble key34 -- The attribute identification information of a scramble key35 -- The information area of application data36 -- The time division frame of ECM data37 --

The time division frame of ECM data38 -- The time division frame of ECM data39 -- The time division frame of ECM data40 -- The time division frame of the enciphered application data A141 -- The time division frame of enciphered application-data A1'42 -- The time division frame of the unenciphered application data A143 -- The time division frame of unenciphered application-data A1'44 [-- Broadcasting station] -- The time division frame of unenciphered application-data A1'45 -- The time division frame of the enciphered application data A146 -- The time division frame of enciphered application-data A1'47 48 [-- A descrambler52 / -- A demultiplexing circuit53 / -- TV monitor54 / -- Multiplexing device in working example 9] -- The transmitting station side device49 -- A transmission line50 -- A receiving side device51

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－168006

(43)公開日　平成９年(1997)６月24日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｌ	9/16			Ｈ０４Ｌ	9/00	６４３	
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｅ	
Ｈ０４Ｈ	1/00			Ｈ０４Ｈ	1/00	Ｆ	
Ｈ０４Ｊ	3/00			Ｈ０４Ｊ	3/00	Ｍ	
Ｈ０４Ｌ	9/36			Ｈ０４Ｌ	9/00	６８５	

審査請求　未請求　請求項の数24　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願平7－326810

(22)出願日　平成７年(1995)12月15日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　栗原　寛
神奈川県横浜市戸塚区戸塚町216番地株式会社日立製作所宇宙技術開発推進本部内

(74)代理人　弁理士　小川　勝男

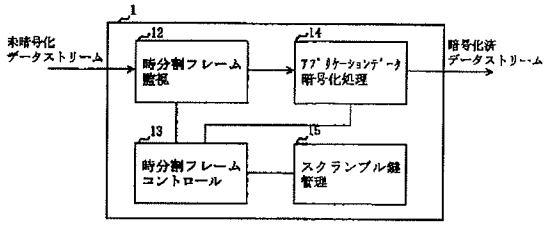
(54)【発明の名称】　通信装置および通信方法

(57)【要約】

【課題】時分割多重化した送信データにスクランブルをかけ、受信端末に伝送する通信ネットワークにおいて、受信側で確実にスクランブルを解くことができる通信装置および通信方法を提供する。

【解決手段】送信側装置のスクランブラは、送信信号と番組関連情報の時分割フレームを時分割多重化した未暗号化データストリームを受けて各時分割フレームを監視し、スクランブル鍵に関する情報を取り出す時分割フレーム監視手段と、スクランブル鍵に関する情報を管理するスクランブル鍵管理手段と、所望のアプリケーションデータにスクランブルをかけるアプリケーションデータ暗号化処理手段と、時分割フレーム監視手段から受けたスクランブル鍵に関する情報に対応するスクランブル鍵をスクランブル鍵管理手段から取得し、送信信号の所望の時分割フレームに対し取得したスクランブル鍵を用いてスクランブルをかけるようアプリケーションデータ暗号化処理手段を制御する時分割フレームコントロール手段を有する。

図１



【特許請求の範囲】
【請求項１】少なくとも１つ以上の送信信号を時分割多重化し、該多重化送信信号の時分割フレームに番組関連情報データの時分割フレームを付した形態の１つの未暗号化データストリームとして出力する多重化手段と、該未暗号化データストリームを受け、該未暗号化データストリームの各時分割フレームを監視し、該時分割フレームに含まれるスクランブル鍵に関する情報を検出する検出手段と、該検出手段で検出した情報に応じたスクランブル鍵を用いて、前記送信信号の所望の時分割フレームに対しスクランブルをかけるスクランブラ手段とを有することを特徴とする通信装置。
【請求項２】前記送信信号がオーディオ、ビデオ、データの何れか１つ又はそれらの組み合わせのアプリケーションデータであり、前記番組関連情報データがスクランブル鍵の情報を含んだＥＣＭデータであることを特徴とする請求項１記載の通信装置。
【請求項３】前記ＥＣＭデータの時分割フレームは、スクランブル鍵の更新切り替え順序を示すバージョンナンバと、該ＥＣＭデータの時分割フレームの伝送情報が有効であるか否かを示す情報インジケータと、時分割フレームＩＤとを含み、前記スクランブラ手段は、前記多重化手段から出力された未暗号化データストリームを受けて各時分割フレームのＩＤを監視し、該時分割フレームＩＤから前記ＥＣＭデータの時分割フレームを検出して前記バージョンナンバ及び前記情報インジケータを取り出す時分割フレーム監視手段と、前記バージョンナンバとスクランブル鍵に関する情報を対応させて管理するスクランブル鍵管理手段と、所望のアプリケーションデータの時分割フレームに対しスクランブルをかけるアプリケーションデータ暗号化処理手段と、前記時分割フレーム監視手段で取り出した前記情報インジケータと前記バージョンナンバを受け、該情報インジケータが有効であるときの該バージョンナンバの連続的な変化をもってスクランブル鍵の切替えを検出し、前記スクランブル鍵管理手段の管理情報に基づき該バージョンナンバに対応するスクランブル鍵情報をもって、所望のアプリケーションデータの時分割フレームに対してスクランブルをかけるよう前記アプリケーションデータ暗号化処理手段を制御する時分割フレームコントロール手段を有することを特徴とする請求項２記載の通信装置。
【請求項４】前記アプリケーションデータの時分割フレームは、運用時に必要となるスクランブル鍵の属性識別情報と、時分割フレームＩＤとを含み、前記スクランブラ手段は、前記多重化手段から出力された未暗号化データストリームを受けて各時分割フレームのＩＤを監視し、該時分割フレームＩＤからアプリケーションデータの時分割フレームを検出して前記スクランブル鍵の属性識別情報を取り出す時分割フレーム監視手段と、スクランブル鍵の情報を管理するスクランブル鍵管理手段と、アプリケーションデータの所望の時分割フレームに対しスクランブルをかけるアプリケーションデータ暗号化処理手段と、前記時分割フレーム監視手段で取り出した該スクランブル鍵の属性識別情報を受け、該スクランブル鍵の属性識別情報の変化をもってスクランブル鍵の切替えを検出し、前記スクランブル鍵管理手段のスクランブル鍵情報に基づきスクランブル鍵を切り替えて、所望のアプリケーションデータの時分割フレームに対してスクランブルをかけるよう前記アプリケーションデータ暗号化処理手段を制御する時分割フレームコントロール手段を有することを特徴とする請求項２記載の通信装置。
【請求項５】少なくとも１つ以上のアプリケーションデータを時分割多重化し、該多重化アプリケーションデータの時分割フレームにスクランブル鍵の情報を含んだＥＣＭデータの時分割フレームを付した形態の１つの未暗号化データストリームとして出力する多重化手段と、該未暗号化データストリームを受け、該未暗号化データストリームの各時分割フレームを監視し、ＥＣＭデータの時分割フレームに含まれる情報からスクランブル鍵の切替えを検出し、該検出した情報に対応したスクランブル鍵を用いて前記アプリケーションデータの所望の時分割フレームに対しスクランブルをかけるスクランブラ手段と、外部入力インターフェイスをもち、該外部入力インターフェイスから入力された情報に基づいてスクランブル鍵情報を切り替えてＥＣＭデータを作成し、前記多重化手段へ送出する鍵切替制御手段とを備え、前記鍵切替制御手段は、スクランブル鍵発生手段と、ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理手段と、ＥＣＭスケジュール管理手段と、タイマと、ＥＣＭ作成手段を有し、スクランブル鍵発生手段は、スクランブル鍵を必要な数だけ発生させ、ＥＣＭスケジュール管理手段は、外部入力インターフェイスをもち、該外部入力インターフェイスからアプリケーションデータとＥＣＭデータの時分割フレームＩＤおよびスクランブル鍵更新切替間隔を入力し、入力した前記アプリケーションデータと前記ＥＣＭデータの時分割フレームＩＤを対応づけて管理し、ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理手段は、前記スクランブル鍵発生手段において発生させたスクランブル鍵それぞれに更新切替え順序をあらわすバージョンナンバおよびスクランブル鍵の属性識別情報を付したものを、前記ＥＣＭスケジュール管理手段から受けたＥＣＭデータの時分割フレームＩＤとアプリケーションデータの時分割フレームＩＤに対応づけて登録管理するとともに、該管理情報を前記スクランブラ手段のスクランブル鍵管理手段に渡し、タイマは、前記ＥＣＭスケジュール管理手段の外部入力インターフェイスから入力された更新間隔を管理し、ＥＣＭ作成手段は、前記ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理手段で登録管理している情報を受けてＥＣＭデータを作成し、前記タイマからのスクランブル鍵更新切替タイミングに従っ

て前記スクランブル鍵の情報を切り替えて前記多重化手段に送出し、前記スクランブラ手段は、時分割フレーム監視手段と、スクランブル鍵管理手段と、アプリケーションデータ暗号化処理手段と、時分割フレームコントロール手段を有し、前記時分割フレーム監視手段は前記多重化手段から出力された未暗号化データストリームを受けて各時分割フレームのＩＤを監視し、該時分割フレームＩＤからＥＣＭデータの時分割フレームを検出して前記バージョンナンバおよび前記情報インジケータを取り出し、前記スクランブル鍵管理手段は、前記ＥＣＭ時分割フレームＩＤースクランブル鍵管理手段から受けたスクランブル鍵に関する情報を管理し、前記時分割フレームコントロール手段は、前記時分割フレーム監視手段で取り出した該情報インジケータと該バージョンナンバを受け、該情報インジケータが有効であるときの該バージョンナンバの連続的な変化をもってスクランブル鍵の切替えを検出し、前記スクランブル鍵管理手段の管理情報に基づき該バージョンナンバに対応するスクランブル鍵情報をもって所望のアプリケーションデータの時分割フレームに対してスクランブルをかけるよう前記アプリケーションデータ暗号化処理手段を制御し、前記アプリケーションデータ暗号化処理手段は前記時分割フレームコントロール手段から受けたスクランブル鍵情報をもって所望のアプリケーションデータの時分割フレームに対してスクランブルをかけるとともに、該アプリケーションデータの時分割フレームの任意の領域に該スクランブル鍵の属性識別情報を書き込むことを特徴とする通信装置。

【請求項６】少なくとも１つ以上のアプリケーションデータを時分割多重化し、該多重化アプリケーションデータの時分割フレームにスクランブル鍵の情報を含んだＥＣＭデータの時分割フレームを付した形態の１つの未暗号化データストリームとして出力する多重化手段と、外部入力インターフェイスをもち、該外部入力インターフェイスから入力されたスクランブル鍵の更新切替間隔を、所望のアプリケーションデータの時分割フレーム毎に管理するとともに、該更新切替間隔に基づいてスクランブル鍵の属性識別情報を切り替えて、前記多重化手段から出力された未暗号化データストリームの所定のアプリケーションデータの時分割フレームに付加する機能をもつ属性識別情報付加機能付きタイマと、前記属性識別情報付加機能付きタイマから出力された該未暗号化データストリームを受け、該未暗号化データストリームの各時分割フレームを監視し、アプリケーションデータの時分割フレームに含まれる情報からスクランブル鍵の切替えを検出し、該検出した情報に対応したスクランブル鍵を用いて所望のアプリケーションデータの時分割フレームに対しスクランブルをかけるスクランブラ手段と、外部入力インターフェイスをもち、該外部入力インターフェイスから入力された情報に基づいてスクランブル鍵情報を切り替えてＥＣＭデータを作成し、前記多重化手段へ送出する鍵切替制御手段とを備え、前記鍵切替制御手段は、スクランブル鍵発生手段と、ＥＣＭ時分割フレームＩＤースクランブル鍵管理手段と、ＥＣＭスケジュール管理手段と、ＥＣＭ作成手段を有し、前記スクランブル鍵発生手段は、スクランブル鍵を必要な数だけ発生させ、前記ＥＣＭスケジュール管理手段は、外部入力インターフェイスをもち、該外部入力インターフェイスからアプリケーションデータとＥＣＭデータの時分割フレームＩＤを入力し、入力した前記アプリケーションデータと前記ＥＣＭデータの時分割フレームＩＤを対応づけて管理し、前記ＥＣＭ時分割フレームＩＤースクランブル鍵管理手段は、前記スクランブル鍵発生手段で発生させたスクランブル鍵を受けて、ＥＣＭスケジュール管理手段から受けたＥＣＭデータの時分割フレームＩＤとアプリケーションデータの時分割フレームＩＤに対応させて登録管理するとともに、該管理情報を前記スクランブラ手段のスクランブル鍵管理手段に渡し、ＥＣＭ作成手段は、前記ＥＣＭ時分割フレームＩＤースクランブル鍵管理手段で登録管理している情報を受けてＥＣＭデータを作成し、前記タイマからのスクランブル鍵更新切替タイミングに従って前記スクランブル鍵の情報を切り替えて多重化手段に送出し、前記スクランブラ手段は、時分割フレーム監視手段と、スクランブル鍵管理手段と、アプリケーションデータ暗号化処理手段と、時分割フレームコントロール手段を有し、前記時分割フレーム監視手段は前記多重化手段から出力された未暗号化データストリームを受けて各時分割フレームのＩＤを監視し、該時分割フレームＩＤからアプリケーションデータの時分割フレームを検出して前記スクランブル鍵の属性識別情報を取り出し、前記スクランブル鍵管理手段は、前記時分割フレームＩＤースクランブル鍵管理手段から受けたスクランブル鍵の情報を管理し、前記時分割フレームコントロール手段は、前記時分割フレーム監視手段で取り出した該スクランブル鍵の属性識別情報を受け、該スクランブル鍵の属性識別情報の変化をもってスクランブル鍵の切替えを検出し、前記スクランブル鍵管理手段のスクランブル鍵情報に基づきスクランブル鍵を切替えて、所望のアプリケーションデータの時分割フレームに対してスクランブルをかけるよう前記アプリケーションデータ暗号化処理部を制御し、前記アプリケーションデータ暗号化手段は、前記時分割フレームコントロール手段から受けたスクランブル鍵に関する情報に対応するスクランブル鍵を用いてスクランブルを施すことを特徴とする通信装置。

【請求項７】請求項５記載の通信装置における鍵切替制御手段の持つ機能と、スクランブラ手段の持つ機能とを１つに合わせ持った鍵切替制御用スクランブラ手段を有し、スクランブル鍵の情報の入力、管理、ＥＣＭデータの作成等を前記鍵切替制御用スクランブラ手段内で行う

ことを特徴とする通信装置。

【請求項8】請求項6記載の通信装置における鍵切替制御手段の持つ機能と、スクランブラ手段の持つ機能と、属性情報付加機能付きタイマの持つ機能とを1つに合わせ持った鍵切替制御用スクランブラ手段を有し、スクランブル鍵の情報の入力、管理、ＥＣＭデータの作成、スクランブル鍵の更新切替間隔の管理、所望のアプリケーションデータの時分割フレームへのスクランブル鍵の属性識別情報の付加等を前記鍵切替制御用スクランブラ手段内で行うことを特徴とする通信装置。

【請求項9】請求項5記載の通信装置において、スクランブラ手段の持つ機能を多重化手段の機能として多重化手段本来の機能に追加し、時分割フレームの監視、スクランブル鍵に関する情報の検出、スクランブル等を前記多重化手段内で行うことを特徴とする通信装置。

【請求項10】請求項6記載の通信装置において、属性情報付加機能付きタイマの持つ機能と、スクランブラ手段の持つ機能を、多重化手段の機能として多重化手段本来の機能に追加し、スクランブル鍵の更新切替間隔の管理、所望のアプリケーションデータの時分割フレームへのスクランブル鍵の属性識別情報の付加、時分割フレームの監視、スクランブル鍵に関する情報の検出、スクランブル等を前記多重化手段内で行うことを特徴とする通信装置。

【請求項11】請求項5記載の通信装置において、鍵切替制御手段のもつ機能と、スクランブラ手段のもつ機能を合わせて多重化手段の機能として多重化手段本来の機能に追加し、鍵切替制御、スクランブル等を前記多重化手段内で行うことを特徴とする通信装置。

【請求項12】請求項6記載の通信装置において、鍵切替制御手段のもつ機能と、スクランブラ手段のもつ機能と、属性識別情報付加機能付きタイマのもつ機能を合わせて多重化手段の機能として多重化手段本来の機能に追加し、鍵切替制御、所望のアプリケーションデータへのスクランブル鍵の属性識別情報の付加、スクランブル等を前記多重化手段内で行うことを特徴とする通信装置。

【請求項13】請求項6記載の通信装置において、属性識別情報付加機能付きタイマの持つ機能を、多重化手段の機能として多重化手段本来の機能に追加し、スクランブル鍵の更新切替間隔の管理、所望のアプリケーションデータの時分割フレームへのスクランブル鍵の属性識別情報の付加等を多重化手段内で行うことを特徴とする通信装置。

【請求項14】少なくとも1つ以上の送信信号を時分割に多重化し、時分割フレームで区切られた1つのデータストリームとして受信側装置へ伝送する通信方法であって、少なくとも1つ以上の送信信号を時分割多重化し、該多重化送信信号の時分割フレームに番組関連情報データの時分割フレームを付した形態の1つの未暗号化データストリームとして出力し、該未暗号化データストリームを受け、該未暗号化データストリームの各時分割フレームを監視し、該時分割フレームに含まれるスクランブル鍵に関する情報を検出し、検出した情報に応じたスクランブル鍵を用いて前記送信信号の所望の時分割フレームに対しスクランブルをかけることを特徴とする通信方法。

【請求項15】前記送信信号がオーディオ、ビデオ、データの何れか1つ又はそれらの組み合わせのアプリケーションデータであり、前記番組関連情報データがスクランブル鍵の情報を含んだＥＣＭデータであることを特徴とする請求項14記載の通信方法。

【請求項16】前記ＥＣＭデータの時分割フレームは、スクランブル鍵の更新切り替え順序を示すバージョンナンバと、該ＥＣＭデータの時分割フレームの伝送情報が有効であるか否かを示す情報インジケータと、時分割フレームＩＤとを含み、時分割多重化された未暗号化データストリームの各時分割フレームのＩＤを監視し、該時分割フレームＩＤからＥＣＭデータの時分割フレームを検出して前記バージョンナンバ及び前記情報インジケータを取り出し、該情報インジケータが有効であるときの該バージョンナンバの連続的な変化をもってスクランブル鍵の切替えを検出し、スクランブル鍵の情報を管理しているスクランブル鍵管理テーブルの管理情報に基づき、該バージョンナンバに対応するスクランブル鍵情報をもって所望の前記アプリケーションデータの時分割フレームに対してスクランブルをかけることを特徴とする請求項15記載の通信方法。

【請求項17】前記アプリケーションデータの時分割フレームは、運用時に必要となるスクランブル鍵の属性識別情報と、時分割フレームＩＤとを含み、時分割多重化して出力された未暗号化データストリームの各時分割フレームのＩＤを監視し、該時分割フレームＩＤからアプリケーションデータの時分割フレームを検出して前記スクランブル鍵の属性識別情報を取り出し、該スクランブル鍵の属性識別情報の変化をもってスクランブル鍵の切替えを検出し、スクランブル鍵の情報を有するスクランブル鍵管理テーブルの鍵情報に基づきスクランブル鍵を切り替えて所望のアプリケーションデータの時分割フレームに対してスクランブルをかけることを特徴とする請求項15記載の通信方法。

【請求項18】少なくとも1つ以上のアプリケーションデータを時分割多重化し、時分割フレームで区切られた1つのデータストリームとして受信側装置へ伝送する通信方法であって、少なくとも1つ以上のアプリケーションデータを時分割多重化し、該多重化アプリケーションデータの時分割フレームにスクランブル鍵の情報を含んだＥＣＭデータの時分割フレームを付した形態の1つの未暗号化データストリームとして出力する多重化ステップと、該未暗号化データストリームを受け、該未暗号化データストリームの各時分割フレームを監視し、ＥＣＭ

データの時分割フレームに含まれる情報からスクランブル鍵の切替えを検出し、該検出した情報に対応したスクランブル鍵を用いてアプリケーションデータの所望の時分割フレームに対しスクランブルをかけるスクランブルステップと、予め設定された情報に基づいてスクランブル鍵情報を切替えてＥＣＭデータを作成し、前記多重化手段へ送出する鍵切替制御ステップからなり、前記鍵切替制御ステップにおいてはスクランブル鍵を必要な数だけ発生させ、発生させたスクランブル鍵それぞれに属性識別情報とバージョンナンバを付して登録管理し、また予め設定されたアプリケーションデータとＥＣＭデータの時分割フレームＩＤとを対応づけて登録管理し、該登録管理情報をスクランブルステップのスクランブル鍵管理テーブルに渡すとともに前記登録管理情報に基づいてＥＣＭデータを作成し、予め設定されたスクランブル鍵の更新間隔に従って前記スクランブル鍵の情報を切り替えて、前記ＥＣＭデータを前記多重化装置ステップに渡す処理を行い、前記スクランブラステップにおいては、前記多重化ステップから出力された未暗号化データストリームを受けて各時分割フレームを監視し、該時分割フレームＩＤからＥＣＭデータの時分割フレームを検出して前記バージョンナンバおよび前記情報インジケータを取り出し、該情報インジケータが有効であるときの該バージョンナンバの連続的な変化をもってスクランブル鍵の切替えを検出し、バージョンナンバとスクランブル鍵情報を対応させて管理しているスクランブル鍵管理テーブルの管理情報に基づき、該バージョンナンバに対応するスクランブル鍵情報をもって所望のアプリケーションデータの時分割フレームに対してスクランブルをかけ、該アプリケーションデータの時分割フレームの任意の領域に該スクランブル鍵の属性識別情報を書き込む処理を行うことを特徴とする通信方法。

【請求項１９】少なくとも１つ以上のアプリケーションデータを時分割多重化し、時分割フレームで区切られた１つのデータストリームとして受信側装置へ伝送する通信方法であって、少なくとも１つ以上のアプリケーションデータを時分割多重化し、該多重化アプリケーションデータの時分割フレームにスクランブル鍵の情報を含んだＥＣＭデータの時分割フレームを付した形態の１つの未暗号化データストリームとして出力する多重化ステップと、予め設定されたスクランブル鍵の更新切替間隔を、所望のアプリケーションデータの時分割フレーム毎に管理するとともに、該更新切替間隔に基づいて鍵の属性識別情報を切替えて、前記未暗号化データストリームの所定のアプリケーションデータの時分割フレームに、鍵の属性識別情報を付加する機能をもつ属性識別情報付加機能付きタイマステップと、該属性識別情報付加機能付きタイマステップから出力された該未暗号化データストリームを受け、該未暗号化データストリームの各時分割フレームを監視し、アプリケーションデータの時分割フレームに含まれる情報からスクランブル鍵の変化を検出し、該検出した情報に対応したスクランブル鍵を用いて前記アプリケーションデータの所望の時分割フレームに対しスクランブルをかけるスクランブルステップと、予め設定された情報に基づいてスクランブル鍵情報を切り替えてＥＣＭデータを作成し、前記多重化手段へ送出する鍵切替制御ステップとからなり、前記鍵切替制御ステップにおいては、スクランブル鍵を必要な数だけ発生させ、発生させたスクランブル鍵と予め設定されたアプリケーションデータとＥＣＭデータの時分割フレームＩＤを対応づけて登録管理し、該登録管理している情報をスクランブラステップのスクランブル鍵管理テーブルに渡すとともに、該登録管理情報に基づいてＥＣＭデータを作成し、予め設定されたスクランンブル鍵更新切替間隔に従って前記スクランブル鍵の情報を切り替えて前記ＥＣＭデータを前記多重化装置ステップに渡す処理を行い、スクランブラステップにおいては、属性識別情報付加機能付きタイマステップから出力された未暗号化データストリームを受けて各時分割フレームのＩＤを監視し、該時分割フレームＩＤからアプリケーションデータの時分割フレームを検出して前記スクランブル鍵の属性識別情報を取り出し、該スクランブル鍵の属性識別情報の変化をもってスクランブル鍵の切替えを検出し、スクランブル鍵の情報を有するスクランブル鍵管理テーブルのスクランブル鍵情報に基づきスクランブル鍵を切替えて所望のアプリケーションデータの時分割フレームに対してスクランブルをかける処理を行うことを特徴とする通信方法。

【請求項２０】１つ以上の送信側装置と１つ以上の受信側装置を有する通信システムにおいて、送信側装置は、少なくとも１つ以上の送信信号を時分割多重化し、該多重化送信信号の時分割フレームに番組関連情報データの時分割フレームを付した形態の１つの未暗号化データストリームとして出力する多重化手段と、該未暗号化データストリームを受け、該未暗号化データストリームの各時分割フレームを監視し、該時分割フレームに含まれるスクランブル鍵に関する情報を検出する手段と、該検出手段で検出した情報に応じたスクランブル鍵を用いて、前記送信信号の所望の時分割フレームに対しスクランブルをかけ、暗号化済データストリームとして出力するスクランブラ手段とを有し、受信側装置は、前記送信側装置から送られてくる暗号化済データストリームを受信し、前記スクランブル鍵に対応するデスクランブル鍵を用いてデスクランブルするデスクランブラ手段と、該デスクランブルしたデータストリームを受け、送信信号ごとに分離する多重分離手段と、該分離した信号を表示する表示手段とを有することを特徴とする通信システム。

【請求項２１】少なくとも１つ以上の送信信号を時分割に多重化した多重化送信信号の時分割フレームに、番組関連情報データの時分割フレームを付した、時分割フレ

ームが連続する形態の１つの未暗号化データストリーム上の所望の送信信号の時分割フレームに対しスクランブルをかけて伝送する通信方法であって、前記連続する時分割フレーム内の第１の時分割フレームに含まれるスクランブル鍵に関する情報の変化に対応してスクランブル鍵を切替え、該第１の時分割フレームの後に続く第２の時分割フレームに対し、前記スクランブル鍵を用いてスクランブルを施すことを特徴とする通信方法。

【請求項２２】前記送信信号がオーディオ、ビデオ、データの何れか１つ又はそれらの組み合わせのアプリケーションデータであり、前記番組関連情報データがスクランブル鍵の情報を含んだＥＣＭデータであることを特徴とする請求項２１記載の通信方法。

【請求項２３】前記第１の時分割フレームはＥＣＭデータの時分割フレーム、前記第２の時分割フレームは前記ＥＣＭデータの時分割フレームに対応するアプリケーションデータの時分割フレームであり、前記ＥＣＭデータの時分割フレームは、スクランブル鍵の更新切り替え順序を示すバージョンナンバと、該ＥＣＭデータの時分割フレームの伝送情報が有効であるか否かを示す情報インジケータとを含み、前記スクランブル鍵に関する情報の変化として、前記情報インジケータが有効であるときの前記バージョンナンバの連続的な変化を用いることを特徴とする請求項２２記載の通信方法。

【請求項２４】前記第１の時分割フレームはアプリケーションデータの時分割フレーム、第２の時分割フレームは該アプリケーションデータの時分割フレームおよび該アプリケーションデータの時分割フレームと対応づけられたアプリケーションデータの時分割フレームであり、前記アプリケーションデータの時分割フレームは、スクランブル鍵の属性識別情報を含み、前記スクランブル鍵に関する情報の変化として、前記アプリケーションデータの時分割フレームに含まれる前記スクランブル鍵の属性識別情報の変化を利用することを特徴とする請求項２２記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、多重化送信信号を受信端末へ伝送する放送システムあるいは通信システムのうち秘匿性を要するシステムに関し、特に、パソコン通信システムやパソコンによる映像配信システム、ＣＡＴＶシステム、地上波放送システム、衛星放送システム、衛星通信システム等において、秘匿化のためにアプリケーションデータにかけるスクランブル鍵の切替えタイミングとスクランブル鍵の情報を含んだ時分割フレームの送信切替えとの同期を、確実になし得る通信装置および通信方法に関する。

【０００２】

【従来の技術】従来、スクランブル鍵の切替えと、それに伴いスクランブル鍵に関する情報を含むエンタイトルメント・コントロール・メッセージ・データ（Entitlement Control Message data：以下ＥＣＭデータと略する）の切替えを行う手法として、次のようなものが知られている。

【０００３】まず多重化手段にＥＣＭデータ専用の入力ポートを備え、ＥＣＭデータは他の入力ポートから入力されるビデオ、オーディオ等のアプリケーションデータよりも時分割フレームへの多重化の優先度を高くしておく。そして、伝送レートは変えずに、各入力ポートから入力されるデータが、時分割多重され多重化手段から出力されるまでの多重化手段内での処理時間が一定となるようにするか、あるいは多重化手段内で必要な処理時間の最大値を設定し、その最大処理時間を一定時間として、スクランブル鍵をスクランブラへ受け渡し、スクランブラにおいてはその一定の処理時間毎に指定されたスクランブル鍵に切替えてスクランブルをかけるようにして、スクランブル鍵の切替えとＥＣＭデータの切替えを行なっている。

【０００４】

【発明が解決しようとする課題】このように、ＥＣＭデータをデータストリームへ多重化するタイミングは多重化手段で決められ、スクランブル鍵の切替えタイミングはスクランブラ内で一定の時間間隔で行われるため、多重化手段へ入力されるアプリケーションデータの組合せ等、何らかの原因により、多重化手段内で設定された一定処理時間に処理が終了せずに一時的にでも乱れが生じると、スクランブル鍵は更新されたにもかかわらず、古いスクランブル鍵の情報を含んだＥＣＭデータを有効なものとして伝送してしまうことがある。そのような場合、受信側ではアプリケーションデータにかかったスクランブルを解くことが不可能となる。このような現象はシステム的にネックであり、受信側ではサービスが一時中断してしまうという問題点があった。

【０００５】また、従来のスクランブル鍵の更新切替手法では、多重化手段とスクランブラ等の手段は独立な仕様をもって各々別々に製造できなかったため、秘匿性を必要としなかった既存伝送路に秘匿性を持たせる場合に、別の仕様の多重化手段が必要となるという欠点もあった。さらに、そのような多重化手段は、高い性能性と厳しい仕様が要求され、価格的にも高価となる。

【０００６】本発明の目的は、スクランブル鍵の切替えとデータストリーム上のスクランブル鍵情報の切替えとを確実に同期させ得る通信装置および通信方法を提供することにある。また、スクランブラ手段と多重化手段とを独立に送信局側設備に備えることができるようにし、既存の秘匿性を必要としなかった伝送路への秘匿性の付加が容易な、融通性の高いシステムの実現を目的としている。

【０００７】

【課題を解決するための手段】これらの目的を達成する

ために、本発明の通信装置は、従来例のように多重化手段内の処理時間を一定にすることによってアプリケーションデータにかけるスクランブルとデータストリーム上のスクランブル鍵に関する情報を同期させるのではなく、多重化後のデータストリーム上でスクランブル鍵情報の更新切替えを検出する手段を設け、検出したスクランブル鍵情報に対応したスクランブル鍵を用いて所望のアプリケーションデータにスクランブルをかけるようにして、アプリケーションデータにかけるスクランブルとスクランブル鍵情報とを同期させる。

【０００８】さらに、上記スクランブラ手段を含む請求項５に記載した通信装置は、スクランブル鍵の切替えを検出するための情報として、多重化後のデータストリームのＥＣＭデータに含まれるバージョンナンバ（スクランブル鍵の更新切替順序を表す）と、情報インジケータ（ＥＣＭデータの伝送情報が有効であるかどうかを示す）を用い、少なくとも１つ以上のアプリケーションデータを時分割多重化したものにＥＣＭデータの時分割フレームを付した形態の１つの未暗号化データストリームとして出力する多重化手段と、多重化手段から出力された未暗号化データストリームを受け、各時分割フレームを監視し、時分割フレームに含まれるスクランブル鍵に関する情報を検出し、検出した情報に対応したスクランブル鍵を用いてアプリケーションデータの所望の時分割フレームに対しスクランブルをかけるスクランブラ手段と、外部入力インターフェイスをもち、外部から入力された情報に基づいてスクランブル鍵情報を切り替えてＥＣＭデータを作成し、多重化手段へ送出する鍵切替制御手段とを備える。

【０００９】このうち鍵切替制御手段は、スクランブル鍵発生手段と、ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理手段と、ＥＣＭスケジュール管理手段と、タイマと、ＥＣＭ作成手段を有し、スクランブル鍵発生手段は、スクランブル鍵を必要な数だけ発生させ、ＥＣＭスケジュール管理手段は、外部入力インターフェイスをもち、外部から入力されたアプリケーションデータとＥＣＭデータの時分割フレームＩＤおよびスクランブル鍵更新切替間隔のうち、アプリケーションデータとＥＣＭデータの時分割フレームＩＤを対応づけて管理する。ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理手段は、スクランブル鍵発生手段で発生させたスクランブル鍵を受け、それぞれにスクランブル鍵の更新切替え順序を表すバージョンナンバと属性識別情報を付したものを登録管理するとともに、その管理情報をスクランブラ手段のスクランブル鍵管理手段に渡す。タイマは、ＥＣＭスケジュール管理手段の外部入力インターフェイスから入力されたスクランブル鍵の更新間隔を管理し、ＥＣＭ作成手段は、ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理手段で登録管理している情報を受けてＥＣＭデータを作成し、タイマからのスクランブル鍵更新切替タイミングに従ってスクランブル鍵の情報を切り替えて多重化装置に送出する。

【００１０】また、スクランブラ手段は、時分割フレーム監視手段と、スクランブル鍵管理手段と、アプリケーションデータ暗号化処理手段と、時分割フレームコントロール手段を有し、時分割フレーム監視手段は多重化手段から出力された未暗号化データストリームを受けて各時分割フレームを監視し、ＥＣＭデータの時分割フレームに含まれるバージョンナンバと情報インジケータを取り出す。時分割フレームコントロール手段は、情報インジケータが有効であるときのバージョンナンバの連続的な変化からスクランブル鍵の切替えの有無を判定するとともにそのバージョンナンバに対応するスクランブル鍵の情報をスクランブル鍵管理手段から取得してアプリケーションデータ暗号化処理手段に渡す。アプリケーションデータ暗号化処理手段は、時分割フレームコントロール手段から受けたスクランブル鍵に関する情報に基づいて所望のアプリケーションデータの時分割フレームにスクランブルをかけるとともに、スクランブルをかけたアプリケーションデータの任意の領域に、スクランブル鍵の属性識別情報を付加する。

【００１１】請求項６に記載した通信装置は、スクランブル鍵の切替えを検出するための情報として、多重化後のデータストリームのアプリケーションデータに含まれるスクランブル鍵の属性識別情報を用い、少なくとも１つ以上のアプリケーションデータを時分割多重化したものにＥＣＭデータの時分割フレームを付した形態の１つの未暗号化データストリームとして出力する多重化手段と、外部入力インターフェイスをもち、外部から入力されたスクランブル鍵の更新切替間隔を、所望のアプリケーションデータの時分割フレーム毎に管理するとともに、スクランブル鍵の属性識別情報をスクランブル鍵の更新切替間隔に基づいて切替えて、多重化装置から出力された未暗号化データストリーム中の所定のアプリケーションデータの時分割フレームに付加する機能をもつ属性識別情報付加機能付きタイマと、属性識別情報付加機能付きタイマから出力された未暗号化データストリームを受け、データストリーム中の時分割フレームに含まれるスクランブル鍵に関する情報を検出し、検出した情報に対応したスクランブル鍵を用いて前記アプリケーションデータの所望の時分割フレームに対しスクランブルをかけるスクランブラ手段と、外部入力インターフェイスをもち、外部から入力された情報に基づいてスクランブル鍵情報を切り替えてＥＣＭデータを作成し、多重化手段へ送出する鍵切替制御手段とを備える。

【００１２】このうち鍵切替制御手段はスクランブル鍵発生手段と、ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理手段と、ＥＣＭスケジュール管理手段と、ＥＣＭ作成手段を有し、スクランブル鍵発生手段は、スクランブル鍵を必要な数だけ発生させ、ＥＣＭスケジュール

管理手段は、外部入力インターフェイスをもち、外部から入力されたアプリケーションデータとＥＣＭデータの時分割フレームＩＤを対応づけて管理する。ＥＣＭ時分割フレームＩＤースクランブル鍵管理手段は、スクランブル鍵発生手段で発生させたスクランブル鍵を受けてＥＣＭスケジュール管理手段からうけたＥＣＭデータの時分割フレームＩＤとアプリケーションデータの時分割フレームＩＤと対応させて登録管理するとともに、その管理情報をスクランブラ手段のスクランブル鍵管理手段に渡す。ＥＣＭ作成手段は、ＥＣＭ時分割フレームＩＤースクランブル鍵管理手段で登録管理している情報を受けてＥＣＭデータを作成し、スクランブル鍵更新切替間隔を管理する属性識別情報付加機能付きタイマからのスクランブル鍵更新切替タイミングに従って前記スクランブル鍵の情報を切替えて多重化装置に送出する。

【００１３】また、スクランブラ手段は、時分割フレーム監視手段と、スクランブル鍵管理手段と、アプリケーションデータ暗号化処理手段と、時分割フレームコントロール手段を有し、時分割フレーム監視手段は多重化手段から出力された未暗号化データストリームを受けて各時分割フレームを監視し、アプリケーションデータの時分割フレームに含まれるスクランブル鍵の属性識別情報を取り出す。時分割フレームコントロール手段は、該スクランブル鍵の属性識別情報の変化からスクランブル鍵の切替えの有無を判定するとともにスクランブル鍵の情報をスクランブル鍵管理手段から取得してアプリケーションデータ暗号化処理手段に渡し、アプリケーションデータ暗号化処理手段は、時分割フレームコントロール手段から受けたスクランブル鍵に関する情報に基づいて所望のアプリケーションデータの時分割フレームにスクランブルをかける。

【００１４】

【発明の実施の形態】本発明の実施の形態について、以下に複数の実施例を挙げて述べる。

【００１５】実施例１

まず、多重化データストリーム上のＥＣＭデータの時分割フレームに含まれるバージョンナンバと情報インジケータから、スクランブル鍵の切替えを検出する第１の実施例について述べる。ここで、多重化データストリームとしては、例えば、ＭＰＥＧ－１　ＳＹＳＴＥＭＳ（ISO/IEC 11172-1）やＭＰＥＧ－２　ＳＹＳＴＥＭＳ（ISO/IEC 13818-1）に記述されているものがある。スクランブル鍵とは、例えば有料スクランブル放送ネットワークにおける鍵配置でいうところのセッション鍵に相当する。また、時分割フレーム、時分割フレームＩＤ、バージョンナンバ、情報インジケータは、同ＭＰＥＧ－２　ＳＹＳＴＥＭＳに記述されているトランスポートパケット（ＴＳＰ：Transport Stream Packet）、パケット識別子（ＰＩＤ：Packet Identifier）、プログラム仕様情報（ＰＳＩ：Program Specific Information）等のバージョンナンバ（version number）、ＰＳＩ等のカレント・ネクスト・アイデンティファイア（current next identifier）にそれぞれ相当し、バージョンナンバはスクランブル鍵の更新切替順に付与する値であり、情報インジケータはそのＥＣＭデータに含まれる情報が有効であるか無効であるかを示す値である。

【００１６】図１は、本発明における鍵切替検出機能をもつスクランブラである。図１において、１はスクランブラ、１２は時分割フレーム監視回路、１３は時分割フレームコントローラ、１４はアプリケーションデータ暗号化処理回路、１５はスクランブル鍵管理テーブルである。

【００１７】スクランブラへの入力は、多重化装置において少なくとも１つのアプリケーションデータを時分割に多重化し、スクランブル鍵の情報を含んだＥＣＭデータの時分割フレームを付して出力された未暗号化データストリームである。スクランブラへ入力された未暗号化データストリームは、入力時の時分割フレーム順に時分割フレーム監視回路に入力される。時分割フレーム監視回路においては、未暗号化データストリームの各時分割フレームの所定の領域に存在する時分割フレームのＩＤを監視する。そして時分割フレームＩＤからＥＣＭデータの時分割フレームを検出し、そのＥＣＭデータに含まれるバージョンナンバと、情報インジケータを取得し、ＥＣＭデータの時分割フレームＩＤとともに時分割フレームコントローラに渡す。時分割フレームコントローラは、時分割フレーム監視回路から受け取ったバージョンナンバを前回のバージョンナンバと比較し、情報インジケータが有効であり、かつバージョンナンバが連続的に変化したときスクランブル鍵が更新され切替わったことを検出する。時分割フレームコントローラは、時分割フレーム監視回路から受け取ったＥＣＭデータの時分割フレームＩＤとバージョンナンバに基づいて、スクランブル鍵管理テーブルからバージョンナンバに対応するスクランブル鍵と、スクランブル鍵の属性識別情報、スクランブルをかける対象アプリケーションデータの時分割フレームＩＤを取得し、その情報をアプリケーションデータ暗号化処理回路に渡す。アプリケーションデータ暗号化処理回路は、その情報を受け、所望するアプリケーションデータの時分割フレームに対し受け取ったスクランブル鍵を用いてスクランブルをかけ、そのアプリケーションデータの時分割フレームの領域内に鍵の属性識別情報を書き込み、暗号化済みデータストリームとして出力する。スクランブルをかけないアプリケーションデータの時分割フレームに対しては、時分割フレーム監視回路を介して、時分割フレームコントローラにおいてスクランブルをかけない判定をし、アプリケーションデータ暗号化処理回路においてはスクランブルをかけずにスルーさせる。

【００１８】図２に、図１のスクランブラを含めた送信

側装置の主要部分の構成図を示す。図2において、1はスクランブラ、2は鍵切替制御装置、3は多重化装置、12は時分割フレーム監視回路、13は時分割フレームコントローラ、14はアプリケーションデータ暗号化処理回路、15はスクランブル鍵管理テーブル、16は暗号化回路、17はECM作成回路、18はタイマ、19はECM時分割フレームID―スクランブル鍵管理回路、20はECMスケジュール管理回路、21はスクランブル鍵発生回路、22は未暗号化ECM管理回路である。

【0019】図2の鍵切替制御装置において、ECMスケジュール管理回路は、外部入力インターフェイスを持ち、外部から入力されたECMデータの時分割フレームIDとアプリケーションデータの時分割フレームIDと対応づけて管理するとともにその情報をECM作成回路、ECM時分割フレームIDースクランブル鍵管理回路、未暗号化ECM管理回路に渡す。また、外部よりスクランブルをかけるアプリケーションデータ毎に鍵切替の更新間隔を設定し、ここで入力設定された更新間隔をECMデータの時分割フレームIDと対応させてタイマへ渡す。未暗号化ECM管理回路は、外部入力インターフェイスを持ち、外部からECMシンタックスを自由に設定し、外部から入力されたECMシンタックスをECMスケジュール管理回路から入力されたECMデータの時分割フレームIDと対応づけて管理する。一方、スクランブル鍵発生回路においては、前もってECMデータの時分割フレームID別に更新切替数回分のスクランブル鍵を更新切替順に発生させ、発生させたスクランブル鍵を、ECM時分割フレームIDースクランブル鍵管理回路に渡す。 ECM時分割フレームIDースクランブル鍵管理回路は、受け取ったスクランブル鍵に、運用するサービスでのスクランブル伝送方式そのもので必要となるスクランブル鍵の属性識別情報をスクランブル鍵の更新切替順にEven、Odd、Even、OddとあるいはOdd、Even、Odd、Even と交互に付与し、各スクランブル鍵に更新切替順にスクランブル鍵の更新切替順序を表すバージョンナンバを割り当て、これらの情報をECMスケジュール管理回路より受け取ったECMデータの時分割フレームのIDごとにアプリケーションデータの時分割フレームIDの組と対応させて管理する。また、ECM時分割フレームIDースクランブル鍵管理回路は、スクランブラのスクランブル鍵管理テーブルに、ECM時分割フレームIDごとに管理しているこれらのスクランブル鍵に関する情報をスクランブル鍵がアプリケーションデータに対し有効になる前までに渡す。ECM作成回路では、 ECM時分割フレームIDースクランブル鍵管理回路で管理している情報を基にECMデータを作成し、スクランブル鍵の情報については暗号化回路で暗号化を施し多重化装置に送出する。ECMデータのスクランブル鍵に関する情報は、タイマで管理しているスクランブル鍵の更新切替間隔に従って切替える。

【0020】多重化装置においては、図2でデータA1、データA1´、データB1、データC1で示すように、1つ以上のオーディオ、ビデオなどのアプリケーションデータを時分割に多重化し、鍵切替制御装置から送られたECMデータを付して1つの未暗号化データストリームとして出力し、スクランブラに渡す。

【0021】スクランブラの各ブロックの動作については図1において説明した通りであるので、ここでは時分割フレームの構成と多重化データストリームの構成例を示してスクランブラの動作説明を行う。

【0022】まず、図10に、ECMデータの時分割フレームの構成を、図11に、アプリケーションデータの時分割フレームの構成を示す。図10において、30は時分割フレームID、31はバージョンナンバ、32は情報インジケータ、33はスクランブル鍵の情報である。また、斜線で網掛けをして示した33のスクランブル鍵の情報は、鍵切替制御装置の暗号化回路において暗号化が施される部分である。一方図11において、30は時分割フレームID、34はスクランブル鍵の属性識別情報、35はビデオ、オーディオなどのデータが格納されるアプリケーションデータの情報領域である。35の斜線で網掛けをして示した部分は、スクランブラのアプリケーションデータ暗号化処理回路において、スクランブルを施す領域である。各時分割フレームIDはアプリケーションデータおよびECMデータ種毎に1つづつ付与する。図2においては、アプリケーションデータA1、A1´、B1、C1に1つづつ、ECMに1つづつ割り当てられる。図10に示すように、ECMデータの時分割フレームはスクランブル鍵の更新切替え順序を示すバージョンナンバと、そのECMデータの時分割フレームの伝送情報が有効であるか無効であるかを示す情報インジケータと、スクランブル鍵の情報を含む。アプリケーションデータの時分割フレームは、図11に示すように、運用時に必要となるスクランブル鍵の属性識別情報を含む。

【0023】多重化装置においてこれらの時分割フレームを多重化し、多重化後の未暗号化データストリームを受けて、スクランブラは所望のアプリケーションデータの時分割フレームに対しスクランブルをかけ、暗号化済データストリームを出力する。スクランブラへの入力である未暗号化データストリームを図12に、スクランブラからの出力である暗号化済データストリームを図13に示す。図12において、36、37、38、39はECMデータの時分割フレームであり、図13において、31はバージョンナンバ、32は情報インジケータ、34はスクランブル鍵の属性識別情報、40はアプリケーションデータA1の時分割フレーム、41はアプリケーションデータA1´の時分割フレームである。

【００２４】図１２に示す未暗号化データストリームは右側の時分割フレームから順にスクランブラに入力される。スクランブラにおいては時分割フレーム監視回路において各時分割フレームのＩＤを監視し、ＩＤからＥＣＭデータの時分割フレームを検出し、バージョンナンバと情報インジケータを取り出す。ここでは、まず３６の時分割フレームが検出される。時分割フレームコントローラは、時分割フレーム監視回路より受けとった情報インジケータより３６の時分割フレームの伝送情報は無効であり、スクランブル鍵は切替わっていないと判定する。次に時分割フレーム監視回路は３７のＥＣＭデータの時分割フレームを検出する。ここで、前回検出した有効なＥＣＭデータのバージョンナンバがｎ－２であったとする。３７のＥＣＭデータの時分割フレームは、情報インジケータが有効でかつバージョンナンバの変化がｎ－２からｎ－１と連続的であるので、時分割フレームコントローラは、スクランブル鍵が切替わったこと検出し、スクランブル鍵管理テーブルから、このバージョンナンバに基づいてスクランブル鍵と鍵に関する情報を取得する。

【００２５】図１６にスクランブル鍵管理テーブルにおけるスクランブル鍵情報の格納イメージ図を示す。スクランブル鍵管理テーブルは、ＥＣＭデータの時分割フレームＩＤ毎に、スクランブルをかける対象のアプリケーションデータの時分割フレームＩＤと、スクランブル鍵と、バージョンナンバと、スクランブル鍵の属性識別情報を対応させて管理している。時分割フレームコントローラは、ＥＣＭデータの時分割フレームＩＤとバージョンナンバｎ－１をもとに、スクランブル鍵管理テーブルからスクランブルをかける対象アプリケーションデータＡ１、Ａ１´のＩＤと、スクランブル鍵Ｋｎ－１と、スクランブル鍵の属性識別情報Ｏｄｄを取得し、アプリケーションデータ暗号化処理回路に渡す。アプリケーションデータ暗号化処理回路は、アプリケーションデータＡ１、およびＡ１´の時分割フレームに対し受け取ったスクランブル鍵Ｋｎ－１を用いてスクランブルをかけ、スクランブル鍵の属性識別情報Ｏｄｄを対象アプリケーションデータの時分割フレームの任意の領域に書き込む。

【００２６】図１３の暗号化済データストリームにおいて、スクランブルを施されたアプリケーションデータＡ１を４０、Ａ１´を４１で斜線で網掛けをして示す。３４は、アプリケーションデータ暗号化処理回路においてアプリケーションデータの時分割フレーム中に書き込まれたスクランブル鍵の属性識別情報である。同様にして、ＥＣＭ時分割フレーム３８についてもスクランブル鍵をＫｎに切り替えてアプリケーションデータＡ１およびＡ１´にスクランブルをかけ、スクランブル鍵の属性識別情報Ｅｖｅｎを対象アプリケーションデータの時分割フレームの任意の領域に書き込む。以降も同様にしてＥＣＭの時分割フレーム３９を検出してスクランブル鍵の切替えを行う。その結果、図１３に示す暗号化済データストリームにおいては、ＥＣＭデータの時分割フレーム３７、３８、３９を先頭とし、それに続くアプリケーションデータの時分割フレームのうち、そのＥＣＭデータに対応するものに対し、ＥＣＭデータの時分割フレーム３７、３８、３９に含まれたスクランブル鍵の情報を用いてスクランブルが施されている。

【００２７】実施例２

次に第２の実施例について説明する。第２の実施例においては、多重化データストリーム上の所望のアプリケーションデータの時分割フレームに含まれるスクランブル鍵の属性識別情報から、そのアプリケーションデータの時分割フレームに施すスクランブル鍵の切替えを検出する。

【００２８】図３に、第２の実施例における送信側設備の構成図を示す。図３において、図２に示す実施例１との相違点は、図２では鍵切替制御装置内に配置されていたタイマを多重化装置の後に配置し、かつ属性識別情報付加機能を持つ属性識別情報付加機能付きタイマ２３とした点にある。図３において、４は実施例２におけるスクランブラ、５は実施例２における鍵切替制御装置、２４は実施例２における時分割フレーム監視回路、２５は実施例２における時分割フレームコントローラ、２６は実施例２におけるアプリケーションデータ暗号化処理回路、２７は実施例２におけるスクランブル鍵管理テーブル、２８は実施例２におけるＥＣＭ時分割フレームＩＤ―スクランブル鍵管理回路、２９は実施例２におけるＥＣＭスケジュール管理回路である。各ブロックの動作については以下で説明する。その他のブロックは実施例２と同様に動作するため、図２と同じ符号を付す。

【００２９】図３の鍵切替制御装置において、ＥＣＭスケジュール管理回路、未暗号化ＥＣＭ管理回路、スクランブル鍵発生回路、暗号化回路の動作は実施例１と同様である。ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理回路において、実施例２ではスクランブル鍵の属性識別情報は付与しない。またスクランブラの鍵管理テーブルへ渡すデータは、ＥＣＭデータの時分割フレームＩＤと、それに対応するアプリケーションデータの時分割フレームＩＤと、スクランブル鍵の情報である。ＥＣＭ作成回路では、ＥＣＭ時分割フレームＩＤ－スクランブル鍵管理回路で管理している情報を基にＥＣＭデータを作成し多重化装置に送出している。ＥＣＭデータのスクランブル鍵に関する情報は、属性識別情報付加機能付きタイマにおいて所望のアプリケーションデータの時分割フレーム毎に管理しているスクランブル鍵の更新切替間隔に従って切替えており、またスクランブル鍵の情報は暗号化回路で暗号化を施している。

【００３０】第２の実施例において、多重化装置は、１つ以上のオーディオ、ビデオなどのアプリケーションデータを時分割多重化し、鍵切替制御装置から送られたＥ

ＣＭデータの時分割フレームを付して１つの未暗号化データストリームとして出力し、属性識別情報付加機能付きタイマに渡す。

【００３１】属性識別情報付加機能付きタイマは外部入力インターフェイスを持ち、外部から入力したスクランブル鍵の更新切替え間隔とその更新切替間隔を適用するアプリケーションデータの時分割フレームのＩＤを対応させて管理する。そして、多重化装置から受けた未暗号化データストリームの時分割フレームＩＤからアプリケーションデータの時分割フレームを検出し、アプリケーションデータＩＤと対応させて管理している更新切替え間隔に基づいてスクランブル鍵の属性識別情報をＥｖｅｎ、Ｏｄｄ、Ｅｖｅｎ、ＯｄｄとあるいはＯｄｄ、Ｅｖｅｎ、Ｏｄｄ、Ｅｖｅｎ と交互に切替えて、アプリケーションデータの任意の領域に書き込む。

【００３２】スクランブラの動作説明は、図１４、図１５に多重化データストリームの構成例を示して行う。なお、本実施例では、アプリケーションデータＡ１、Ａ１´の組についてのみ述べる。図１４はスクランブラに入力される未暗号化データストリームを示し、４２はアプリケーションデータＡ１の時分割フレーム、４３はアプリケーションデータＡ１´の時分割フレーム、４４はアプリケーションデータＡ１´の時分割フレームである。図１４の未暗号化データストリームは右側の時分割フレームから順にスクランブラに入力される。スクランブラにおいては時分割フレーム監視回路において各時分割フレームのＩＤを監視し、ＩＤからアプリケーションデータの時分割フレームを検出し、時分割フレームＩＤとスクランブル鍵の属性識別情報を取り出す。図１４においては、まず４２のアプリケーションデータＡ１の時分割フレームが検出される。ここで、前回検出したアプリケーションデータＡ１の時分割フレームに含まれていた属性識別情報がＥｖｅｎであったとする。時分割フレームコントローラは、４２の時分割フレームのスクランブル鍵の属性識別情報が前回検出した同じアプリケーションデータの組の時分割フレームの属性識別情報ＥｖｅｎからＯｄｄに切替わっていることよりスクランブル鍵の切替えを検出し、スクランブル鍵管理テーブルから、アプリケーションデータの時分割フレームＩＤに基づいてスクランブル鍵を取得する。図１７に、第２の実施例におけるスクランブル鍵管理テーブルのスクランブル鍵情報の格納イメージ図を示す。スクランブル鍵管理テーブルは、 スクランブルをかける対象のアプリケーションデータの時分割フレームＩＤの組毎に、 ＥＣＭデータの時分割フレームＩＤと、スクランブル鍵を管理する。時分割フレームコントローラは、アプリケーションデータＡ１の時分割フレームＩＤをもとに、スクランブル鍵管理テーブルから、前回用いたスクランブル鍵Ｋｎ－２の次のスクランブル鍵であるＫｎ－１を取得し、アプリケーションデータ暗号化処理回路に渡す。アプリケーションデータ暗号化処理回路は、アプリケーションデータＡ１の時分割フレームに対し受け取ったスクランブル鍵Ｋｎ－１を用いてスクランブルをかける。次に時分割フレーム監視回路は、アプリケーションデータＡ１´の時分割フレーム４３を検出するが、Ａ１´はＡ１と同じスクランブル鍵を適用するアプリケーションデータの組となっており、スクランブル鍵の属性識別情報はＯｄｄのままで切替わっていないため、同じくスクランブル鍵Ｋｎ－１を用いてスクランブルを施す。時分割フレーム監視回路は、同様にして他のアプリケーションデータの時分割フレームをいくつか検出したあと、アプリケーションデータＡ１´の時分割フレーム４４を検出し、時分割フレームコントローラにおいてスクランブル鍵の属性識別情報がＥｖｅｎに切替わっていることを検出し、スクランブル鍵をＫｎに切替えてスクランブルを施す。図１５の暗号化済データストリームにおいて、スクランブルを施されたアプリケーションデータＡ１を４５、Ａ１´を４６で斜線で網掛けをして示す。以下のデータストリーム上においても同様にスクランブル鍵の属性識別情報の変化に基づいてスクランブル鍵を切替える。他のアプリケーションデータの時分割フレームについても同様である。

【００３３】実施例３

図４は、図２の第１の実施例におけるスクランブラと鍵切替制御装置の機能を合わせ持つ鍵切替制御用スクランブラと、多重化装置からなる第３の実施例の送信側装置の構成図である。図４において、６は鍵切替制御用スクランブラである。本実施例では、第１の実施例で鍵切替制御装置が行っていたスクランブル鍵の発生、発生させたスクランブル鍵と外部から入力された情報との対応付けと管理、ＥＣＭデータの作成等と、スクランブラが行っていた時分割フレームの監視、スクランブル鍵に関する情報の検出、検出した情報に基づくスクランブル処理等をすべて鍵切替制御用スクランブラにおいて行う。鍵切替制御用スクランブラ内の各ブロックおよび多重化装置は図２において説明したものと同じ動作をするため、同じ符号をつけてここでは説明を省略する。

【００３４】実施例４

図５は、図３の第２の実施例における属性識別情報付加機能付きタイマとスクランブラと鍵切替制御装置の機能を合わせ持つ鍵切替制御用スクランブラと、多重化装置からなる第４の実施例の送信側装置の構成図である。図５において、７は属性識別情報付加機能付きタイマをもつ鍵切替制御用スクランブラである。本実施例においては、第２の実施例で鍵切替制御装置が行っていたスクランブル鍵の発生、発生させたスクランブル鍵と外部から入力された情報との対応付けと管理、ＥＣＭデータの作成等と、属性識別情報付加機能付きタイマが行っていたスクランブル鍵の属性識別情報のアプリケーションデータの時分割フレームへの付加、スクランブル鍵の更新切

替間隔の制御等と、スクランブラが行っていた時分割フレームの監視、スクランブル鍵に関する情報の検出、検出した情報に基づくスクランブル処理等をすべて属性識別情報付加機能付きタイマをもつ鍵切替制御用スクランブラにおいて行う。属性識別情報付加機能付きタイマをもつ鍵切替制御用スクランブラ内の各ブロックおよび多重化装置は図３において説明したものと同じ動作をするため、同じ符号をつけてここでは説明を省略する。

【００３５】実施例５

図６は、図２の第１の実施例におけるスクランブラの持つ機能を多重化装置の機能として多重化装置が持つ本来の機能に追加した多重化装置と、鍵切替制御装置を有する第５の実施例の送信側装置の構成図である。図６において、８はスクランブル機能をもつ多重化装置である。本実施例においては、第１の実施例で多重化装置が行っていたアプリケーションデータとＥＣＭデータの時分割多重化等と、スクランブラが行っていた時分割フレームの監視、スクランブル鍵に関する情報の検出、検出した情報に基づくスクランブル処理等をスクランブル機能をもつ多重化装置において行う。本実施例のスクランブル機能をもつ多重化装置内の各ブロックおよび鍵切替制御装置は図２において説明したものと同じ動作をするため、同じ符号をつけてここでは説明を省略する。

【００３６】実施例６

図７は、図３の第２の実施例における属性識別情報付加機能付きタイマとスクランブラの持つ機能を、多重化装置の機能として多重化装置が持つ本来の機能に追加した多重化装置と、鍵切替制御装置を有する第６の実施例における送信側装置の構成図である。図７において、９はスクランブル機能と属性識別情報付加機能付きタイマをもつ多重化装置である。本実施例においては、第２の実施例で多重化装置が行っていたアプリケーションデータとＥＣＭデータの時分割多重化等と、属性識別情報付加機能付きタイマが行っていたスクランブル鍵の属性識別情報のアプリケーションデータの時分割フレームへの書き込み、スクランブル鍵の切替間隔の制御等と、スクランブラが行っていた時分割フレームの監視、スクランブル鍵の切替えの検出、スクランブル等をスクランブル機能と属性識別情報付加機能付きタイマをもつ多重化装置において行う。本実施例のスクランブル機能と属性識別情報付加機能付きタイマをもつ多重化装置内の各ブロックおよび鍵切替制御装置は、図３において説明したものと同じ動作をするため、同じ符号をつけてここでは説明を省略する。

【００３７】実施例７

図８は、図２の第１の実施例におけるスクランブラと、鍵切替制御装置の持つ機能を、多重化装置の機能として多重化装置本来の機能に追加した第７の実施例における送信側装置の構成図である。図８において、１０は鍵切替制御機能とスクランブル機能をもつ多重化装置である。本実施例では第１の実施例の鍵切替制御装置が行っていたスクランブル鍵の発生、発生させたスクランブル鍵と外部から入力された情報との対応付けと管理、ＥＣＭデータの作成等と、多重化装置が行っていたアプリケーションデータとＥＣＭデータの時分割多重化等と、スクランブラが行っていた時分割フレームの監視、スクランブル鍵の切替えの検出、スクランブル等を鍵切替制御機能とスクランブル機能をもつ多重化装置において行う。本実施例の鍵切替制御機能とスクランブル機能をもつ多重化装置内の各ブロックは、図２において説明したものと同じ動作をするため、同じ符号をつけてここでは説明を省略する。

【００３８】実施例８

図９は、図３に示す第２の実施例における、属性機能付加機能付きタイマと、スクランブラと、鍵切替制御装置の持つ機能を、多重化装置の機能として多重化装置本来の機能に追加した第８の実施例における送信側装置の構成図である。図９において、１１は鍵切替制御機能と属性識別情報付加機能付きタイマとスクランブル機能をもつ多重化装置である。本実施例では第２の実施例の鍵切替制御装置で行っていたスクランブル鍵の発生、発生させたスクランブル鍵と外部から入力された情報との対応付けと管理、ＥＣＭデータの作成等と、多重化装置が行っていたアプリケーションデータとＥＣＭデータの時分割多重化等と、属性識別情報付加機能付きタイマが行っていたスクランブル鍵の属性識別情報のアプリケーションデータの時分割フレームへの書き込み、スクランブル鍵の切替間隔の制御等と、スクランブラが行っていた時分割フレームの監視、スクランブル鍵の切替えの検出、スクランブル等を鍵切替制御機能と属性識別情報付加機能付きタイマとスクランブル機能をもつ多重化装置において行う。本実施例の鍵切替制御機能と属性識別情報付加機能付きタイマとスクランブル機能をもつ多重化装置内の各ブロックは、図３において説明したものと同じ動作をするため、同じ符号をつけてここでは説明を省略する。

【００３９】実施例９

図１９は、図３に示す第２の実施例における属性識別情報付加機能付きタイマの持つ機能を、多重化装置の機能として多重化装置本来の機能に追加した第９の実施例における送信側装置の構成図である。図１９において、５４は属性識別情報付加機能付きタイマを持つ多重化装置である。本実施例では、第２の実施例の属性識別情報付加機能付きタイマで行っていたスクランブル鍵の更新切替間隔の管理、所望のアプリケーションデータの時分割フレームへのスクランブル鍵の属性識別情報の付加等を属性識別情報付加機能付きタイマを持つ多重化装置において行う。本実施例のスクランブラ、鍵切替制御装置の各ブロックは、図３において説明したものと同じ動作をするため、同じ符号をつけてここでは説明を省略する。

【００４０】また、図示していないが、図２、図４、図６、図８で説明した実施例１、３、５、７における送信側装置は、運用するサービスによってスクランブル鍵の属性識別情報を必要としない実施例も考えられる。その場合は鍵切替制御装置の時分割フレームＩＤースクランブル鍵管理回路において、スクランブル鍵発生回路から受けたスクランブル鍵に属性識別情報を付与しない。また、時分割フレームＩＤースクランブル鍵管理回路からスクランブラのスクランブル鍵管理テーブルに送られる情報は、各ＥＣＭデータの時分割フレームＩＤと、それに対応づけた、アプリケーションデータの時分割フレームＩＤの組、スクランブル鍵の情報、バージョンナンバである。またスクランブラのアプリケーションデータ暗号化処理回路は、アプリケーションデータの時分割フレームにスクランブル鍵の属性識別情報を書き込む機能はもたず、スクランブラから出力されるアプリケーションデータの時分割フレームにはスクランブル鍵の属性識別情報は含まれていない。

【００４１】本発明が適用されるシステムの構成

図１８は、本発明の通信装置を適用する通信システムの構成図である。図１８において、４７は放送局、４８は送信局側装置、４９は伝送路、５０は受信側装置、５１はデスクランブラ、５２は多重分離回路、５３はＴＶモニタである。４８の送信側装置は、ここでは本発明の第１の実施例に示した構成であり、多重化装置３とスクランブラ１と鍵切替制御装置２を有するが、この他の実施例で示した構成であってもよい。放送局等で作成された番組は、ビデオ、オーディオなどのアプリケーションデータからなっており、送信側装置では多重化装置においてこれらのアプリケーションデータを時分割に多重化し、鍵切替制御装置で作成したＥＣＭデータの時分割フレームを付して、１つの未暗号化データストリームとして出力する。スクランブラはこの未暗号化データストリームを受け、ストリーム上の時分割フレームに含まれるスクランブル鍵に関する情報を検出し、検出した情報に対応するスクランブル鍵を用いてスクランブルを施し、暗号化済データストリームを伝送する。このときの伝送方法は、有線、地上波、衛星などを用いる場合が考えられる。受信側装置は、伝送されてきた暗号化済ストリームを受け、デスクランブラにおいて送信側でのスクランブル鍵に対応するデスクランブル鍵を用いてスクランブルを解除し、多重分離回路において多重化されたビデオ、オーディオなどのアプリケーションデータを、それぞれ分離し、ＴＶモニタ等の表示装置でビデオ、オーディオを表示し、放送局で作成した番組を視聴する。

【００４２】実施例の効果

以上に述べた各実施例においては、スクランブル鍵情報の切替えを多重化後のデータストリーム上でスクランブラが検出するようにし、検出したそのデータストリーム上でのスクランブル鍵情報に合わせてスクランブラがスクランブル鍵の切替えを行うことにより、確実にスクランブル鍵の切替えと多重化後のデータストリーム上でのスクランブル鍵情報の切替えとで同期を確立することができる。そのため、スクランブル鍵が更新され切替わったのに古いスクランブル鍵の情報を含んだＥＣＭデータを現時点で有効なものとして伝送したり、その逆になるようなことが防止される。従って受信側装置ではアプリケーションデータにかかったスクランブルを確実に解くことが可能となる。

【００４３】また、従来は、送信側装置においてスクランブル鍵とデータストリーム上に含まれるスクランブル鍵に関する情報との同期が乱れ、受信側でスクランブルが解けずに視聴が不可能となった場合の対策として、伝送されてきた多重化データストリーム上のスクランブル鍵の情報によらずに、別経路で与えられたデスクランブル鍵情報から正しいデスクランブル鍵を検索し、スクランブルを解くといったような機能が受信側装置に設けられている場合があった。本発明によれば、確実にスクランブル鍵の切替えと多重化データストリーム上でのスクランブル鍵情報の切替えとで同期を確立することができるため、そのような余分な機能を受信側装置に持たせる必要がなくなる。

【００４４】さらに、実施例１、実施例２、実施例３、実施例４、実施例９においては、データ送信の秘匿化で必要となる機能を実施例１においてはスクランブラと鍵切替制御装置とで、実施例２においては属性識別情報付加機能付きタイマ、スクランブラと鍵切替制御装置とで、実施例３および４においては鍵切替制御用スクランブラで構成することにより、多重化処理部とは無関係に送信側装置に備えることができる。従って、秘匿性を必要としなかった既存の通信システムへの秘匿性の付加が容易となり、融通性の高いシステムを構成できる。

【００４５】

【発明の効果】本発明の通信装置および通信方法によれば、多重化装置での処理時間とは無関係に、スクランブル鍵情報の変化を多重化後のデータストリーム上でスクランブラが検出するようにし、検出したそのデータストリーム上でのスクランブル鍵情報に対応するスクランブル鍵を用いてスクランブラがスクランブルを行うことにより、確実にスクランブル鍵の切替えと多重化後のデータストリーム上でのスクランブル鍵情報の切替えとで同期を確立することができる。そのため、受信側装置ではアプリケーションデータにかかったスクランブルを確実に解くことが可能となる。

【図面の簡単な説明】

【図１】本発明のスクランブラの図である。

【図２】本発明の１実施例の送信局側装置の図である。

【図３】本発明の１実施例の送信局側装置の図である。

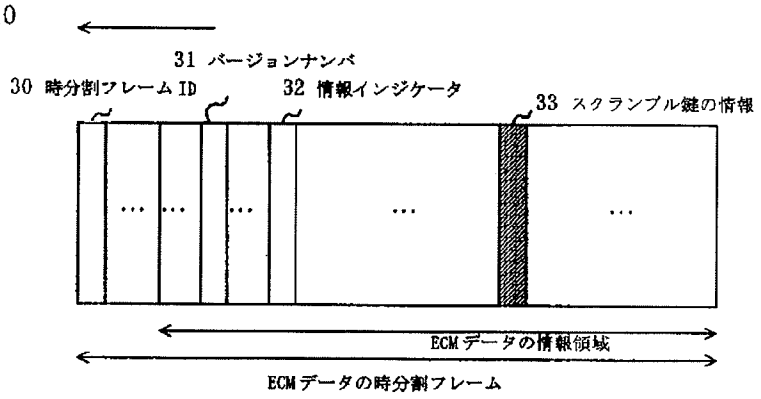
【図４】本発明の１実施例の送信局側装置の図である。

【図５】本発明の１実施例の送信局側装置の図である。

【図６】本発明の１実施例の送信局側装置の図である。
【図７】本発明の１実施例の送信局側装置の図である。
【図８】本発明の１実施例の送信局側装置の図である。
【図９】本発明の１実施例の送信局側装置の図である。
【図１０】ＥＣＭデータの時分割フレームの情報構成例である。
【図１１】アプリケーションデータの時分割フレームの情報構成例である。
【図１２】第１の実施例におけるスクランブラへ入力される未暗号化データストリームの構成例である。
【図１３】第１の実施例におけるスクランブラから出力される暗号化済データストリームの構成例である。
【図１４】第２の実施例におけるスクランブラへ入力される未暗号化データストリームの構成例である。
【図１５】第２の実施例におけるスクランブラから出力される暗号化済データストリームの構成例である。
【図１６】第１の実施例におけるスクランブル鍵管理テーブルのスクランブル鍵とスクランブル鍵に関する情報の格納イメージ図である。
【図１７】第２の実施例におけるスクランブル鍵管理テーブルのスクランブル鍵とスクランブル鍵に関する情報の格納イメージ図である。
【図１８】本発明が適用される通信システム全体の構成図である。
【図１９】本発明の１実施例の送信局側装置の図である。
【符号の説明】
１…スクランブラ、２…鍵切替制御装置、３…多重化装置、４…実施例２におけるスクランブラ、５…実施例２における鍵切替制御装置、６…鍵切替制御用スクランブラ、７…属性識別情報付加機能付きタイマをもつ鍵切替制御用スクランブラ、８…スクランブル機能をもつ多重化装置、９…スクランブル機能と属性識別情報付加機能付きタイマをもつ多重化装置、１０…鍵切替制御機能とスクランブル機能をもつ多重化装置、１１…鍵切替制御機能と属性識別情報付加機能付きタイマとスクランブル機能をもつ多重化装置、１２…時分割フレーム監視回路、１３…時分割フレームコントローラ、１４…アプリケーションデータ暗号化処理回路、１５…スクランブル鍵管理テーブル、１６…暗号化回路、１７…ＥＣＭ作成回路、１８…タイマ、１９…ＥＣＭ時分割フレームＩＤ—スクランブル鍵管理回路、２０…ＥＣＭスケジュール管理回路、２１…スクランブル鍵発生回路、２２…未暗号化ＥＣＭ管理回路、２３…属性識別情報付加機能付きタイマ、２４…実施例２における時分割フレーム監視回路、２５…実施例２における時分割フレームコントローラ、２６…実施例２におけるアプリケーションデータ暗号化処理回路、２７…実施例２におけるスクランブル鍵管理テーブル、２８…実施例２におけるＥＣＭ時分割フレームＩＤ—スクランブル鍵管理回路、２９…実施例２におけるＥＣＭスケジュール管理回路、３０…時分割フレームＩＤ、３１…バージョンナンバ、３２…情報インジケータ、３３…スクランブル鍵の情報、３４…スクランブル鍵の属性識別情報、３５…アプリケーションデータの情報領域、３６…ＥＣＭデータの時分割フレーム、３７…ＥＣＭデータの時分割フレーム、３８…ＥＣＭデータの時分割フレーム、３９…ＥＣＭデータの時分割フレーム、４０…暗号化済アプリケーションデータＡ１の時分割フレーム、４１…暗号化済アプリケーションデータＡ１′の時分割フレーム、４２…未暗号化アプリケーションデータＡ１の時分割フレーム、４３…未暗号化アプリケーションデータＡ１′の時分割フレーム、４４…未暗号化アプリケーションデータＡ１′の時分割フレーム、４５…暗号化済アプリケーションデータＡ１の時分割フレーム、４６…暗号化済アプリケーションデータＡ１′の時分割フレーム、４７…放送局、４８…送信局側装置、４９…伝送路、５０…受信側装置、５１…デスクランブラ、５２…多重分離回路、５３…ＴＶモニタ、５４…実施例９における多重化装置

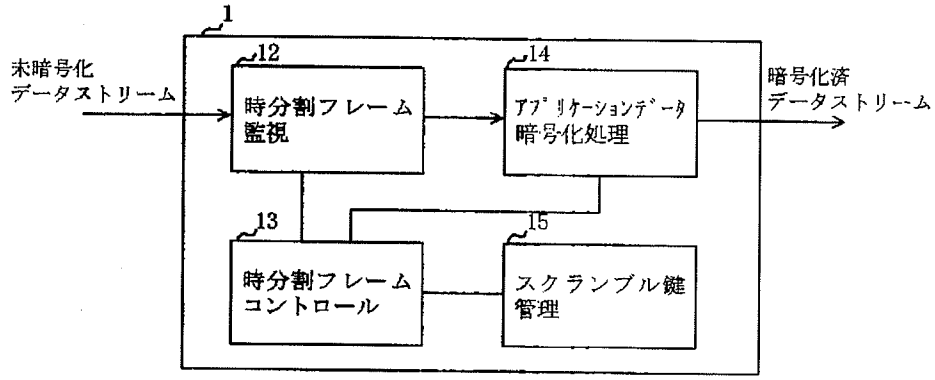
【図１０】

図 10



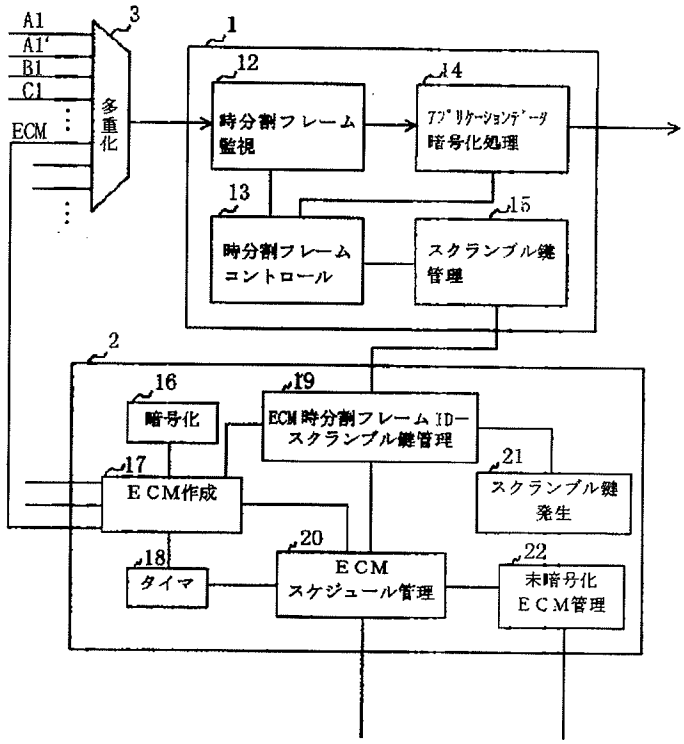
【図１】

図１


1
未暗号化
データストリーム
12
時分割フレーム
監視
14
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀ
暗号化処理
暗号化済
データストリーム
13
時分割フレーム
コントロール
15
スクランブル鍵
管理

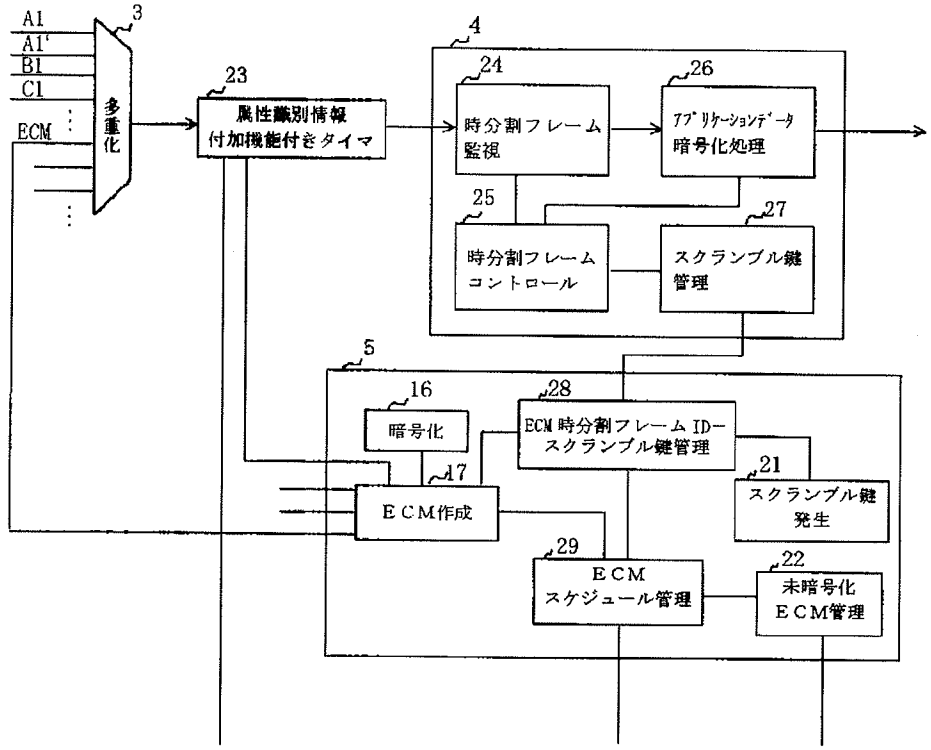
【図２】

図２


A1
A1'
B1
C1
ECM
多重化
3
1
12
時分割フレーム
監視
14
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀ
暗号化処理
13
時分割フレーム
コントロール
15
スクランブル鍵
管理
2
16
暗号化
19
ECM時分割フレームID－
スクランブル鍵管理
17
ECM作成
21
スクランブル鍵
発生
18
タイマ
20
ECM
スケジュール管理
22
未暗号化
ECM管理

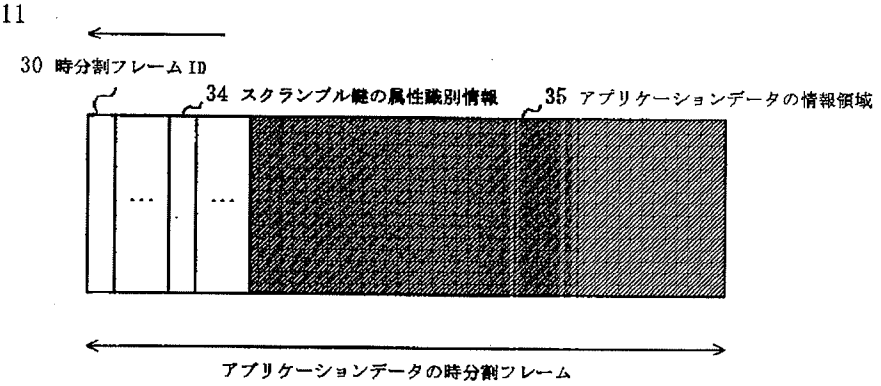
【図３】

図３


A1
A1'
B1
C1
ECM
3
多重化
23
属性識別情報
付加機能付きタイマ
4
24
時分割フレーム
監視
26
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀ
暗号化処理
25
時分割フレーム
コントロール
27
スクランブル鍵
管理
5
16
暗号化
28
ECM時分割フレームID－
スクランブル鍵管理
17
ECM作成
21
スクランブル鍵
発生
29
ECM
スケジュール管理
22
未暗号化
ECM管理

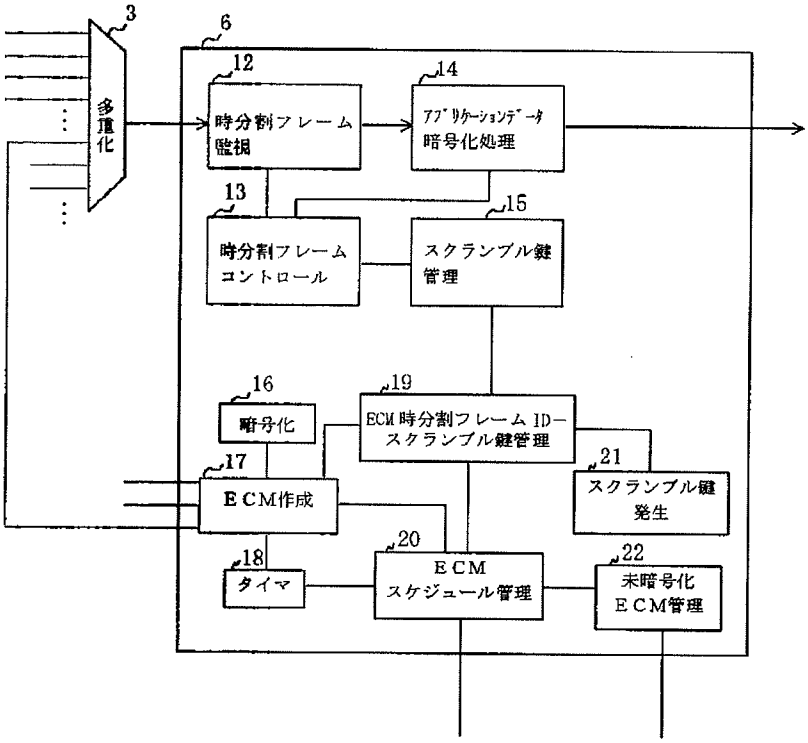
【図１１】

図11


30 時分割フレームID
34 スクランブル鍵の属性識別情報
35 アプリケーションデータの情報領域
アプリケーションデータの時分割フレーム

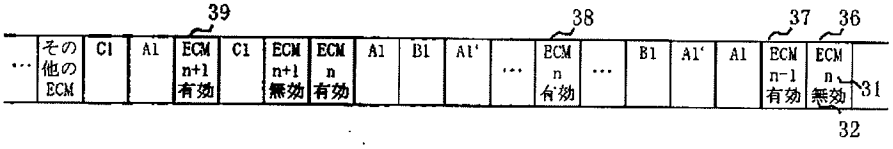
【図４】

図４



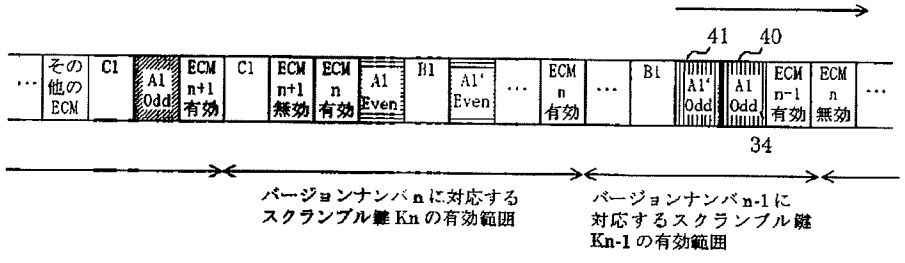
【図１２】

図 12



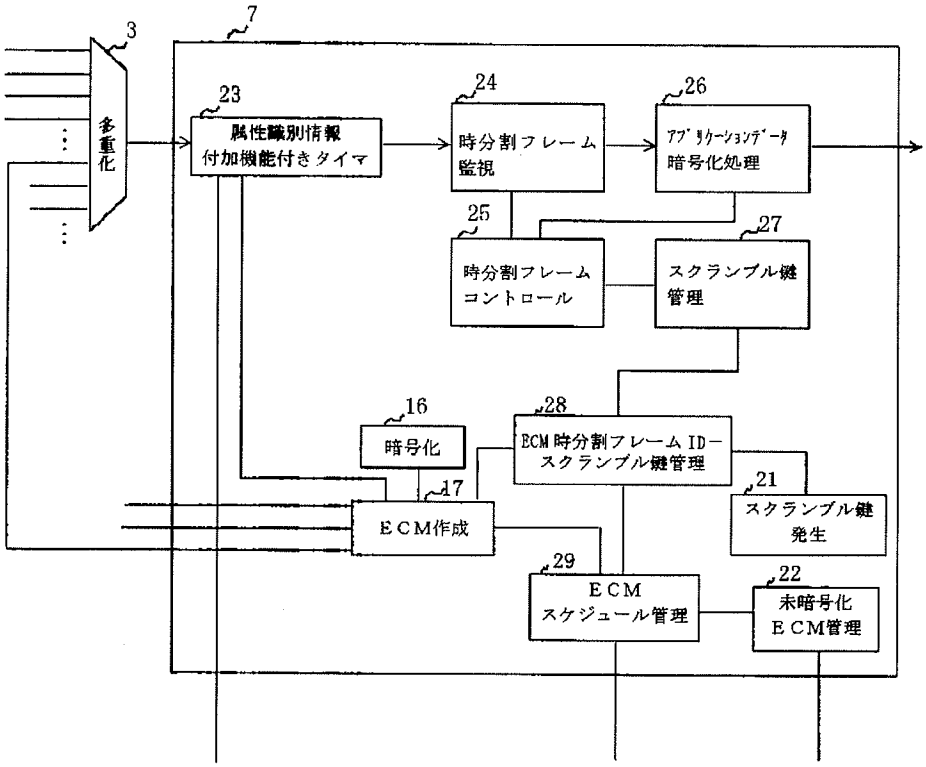
【図１３】

図 13



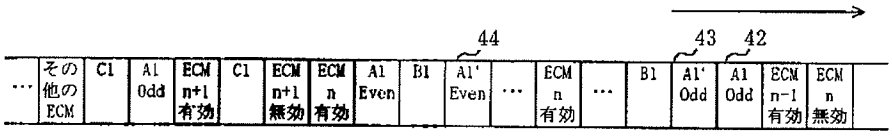
【図5】

図5



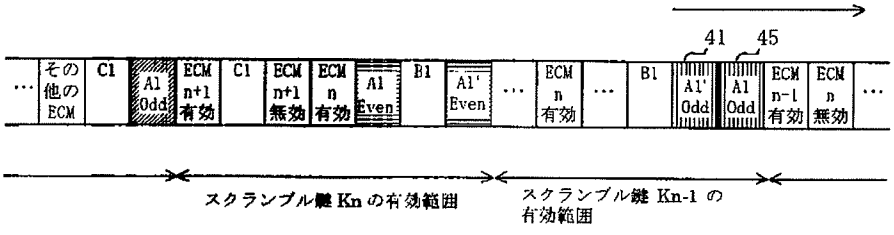
【図14】

図14



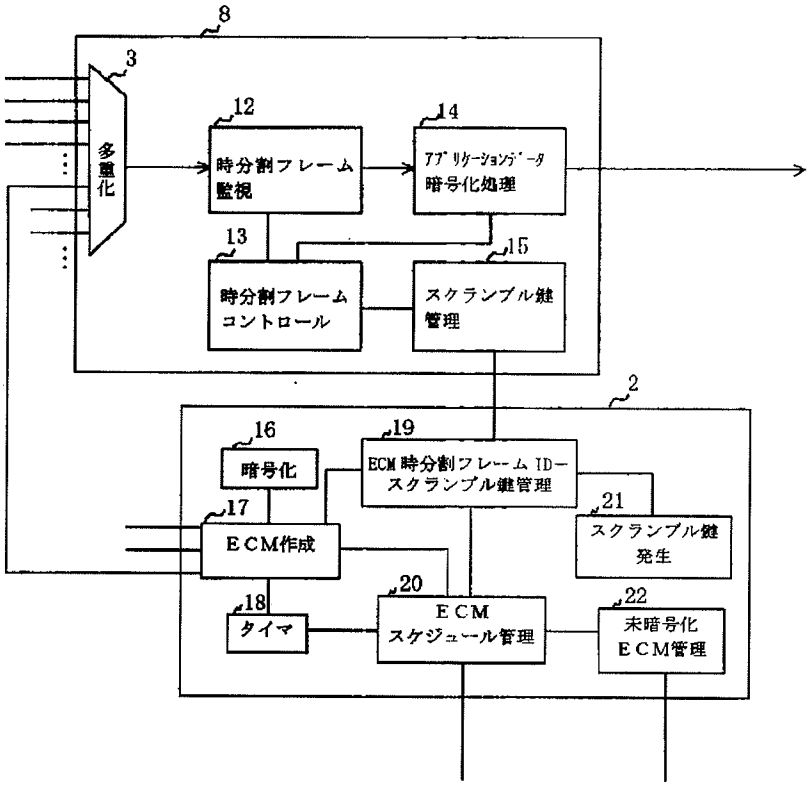
【図15】

図15



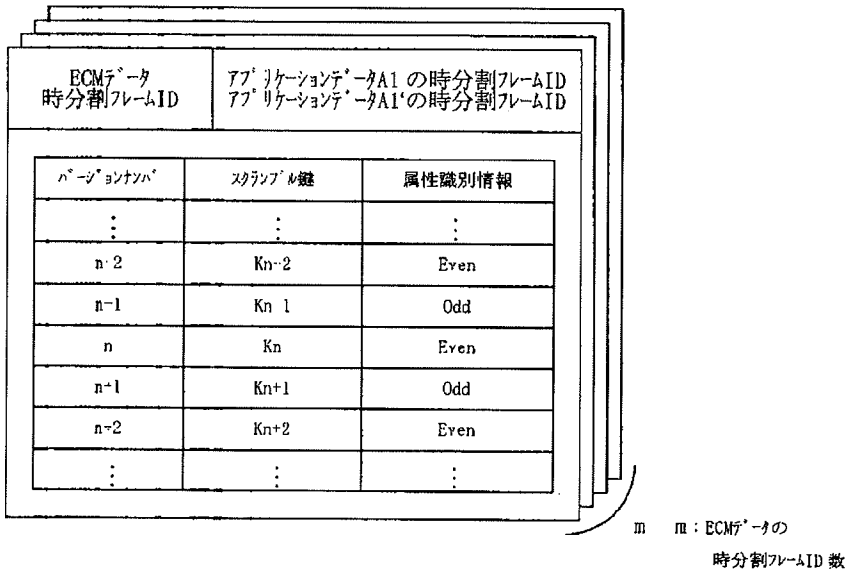
【図6】

図6


8
3
多重化
12
時分割フレーム監視
14
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀ暗号化処理
13
時分割フレームコントロール
15
スクランブル鍵管理
2
16
暗号化
19
ECM時分割フレームID－スクランブル鍵管理
21
スクランブル鍵発生
17
ECM作成
18
タイマ
20
ECMスケジュール管理
22
未暗号化ECM管理

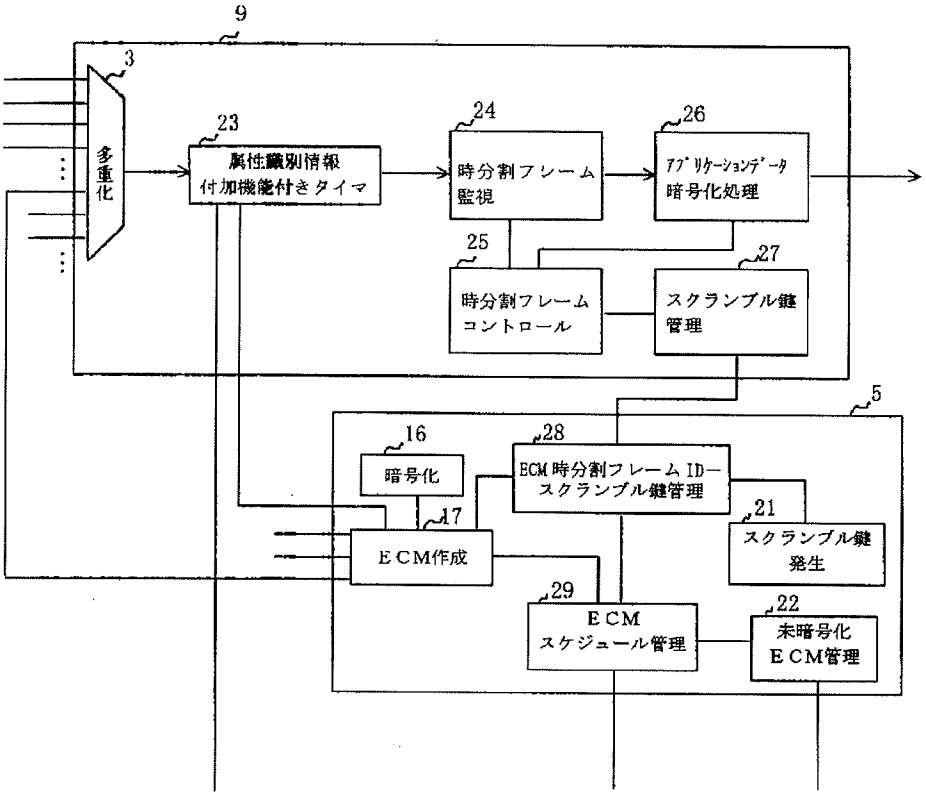
【図16】

図16


ECMﾃﾞｰﾀ時分割ﾌﾚｰﾑID
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀA1の時分割ﾌﾚｰﾑID
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀA1'の時分割ﾌﾚｰﾑID
ﾊﾞｰｼﾞｮﾝﾅﾝﾊﾞ
ｽｸﾗﾝﾌﾞﾙ鍵
属性識別情報
n-2
Kn-2
Even
n-1
Kn-1
Odd
n
Kn
Even
n+1
Kn+1
Odd
n-2
Kn+2
Even
m
m：ECMﾃﾞｰﾀの時分割ﾌﾚｰﾑID数

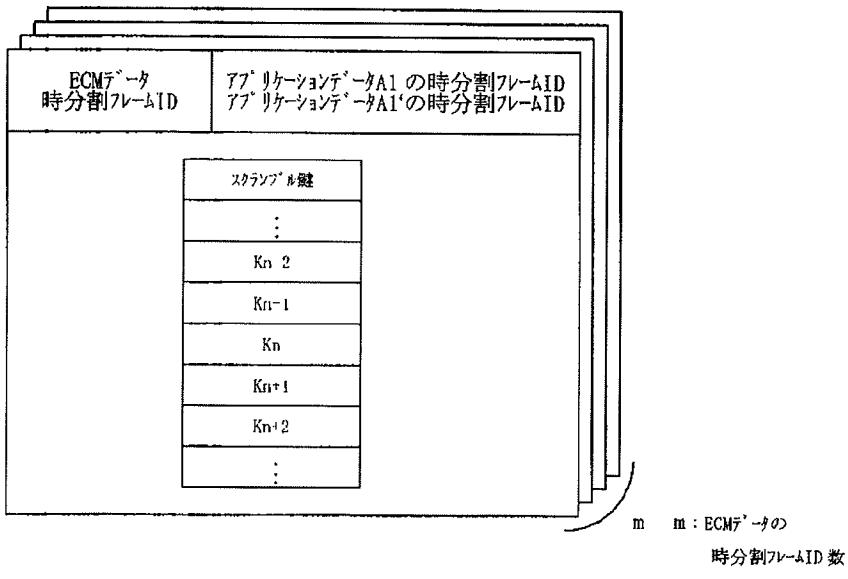
【図7】

図7


9
3
多重化
23
属性識別情報
付加機能付きタイマ
24
時分割フレーム
監視
26
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀ
暗号化処理
25
時分割フレーム
コントロール
27
スクランブル鍵
管理
5
16
暗号化
28
ECM時分割フレームID－
スクランブル鍵管理
17
ＥＣＭ作成
21
スクランブル鍵
発生
29
ＥＣＭ
スケジュール管理
22
未暗号化
ＥＣＭ管理

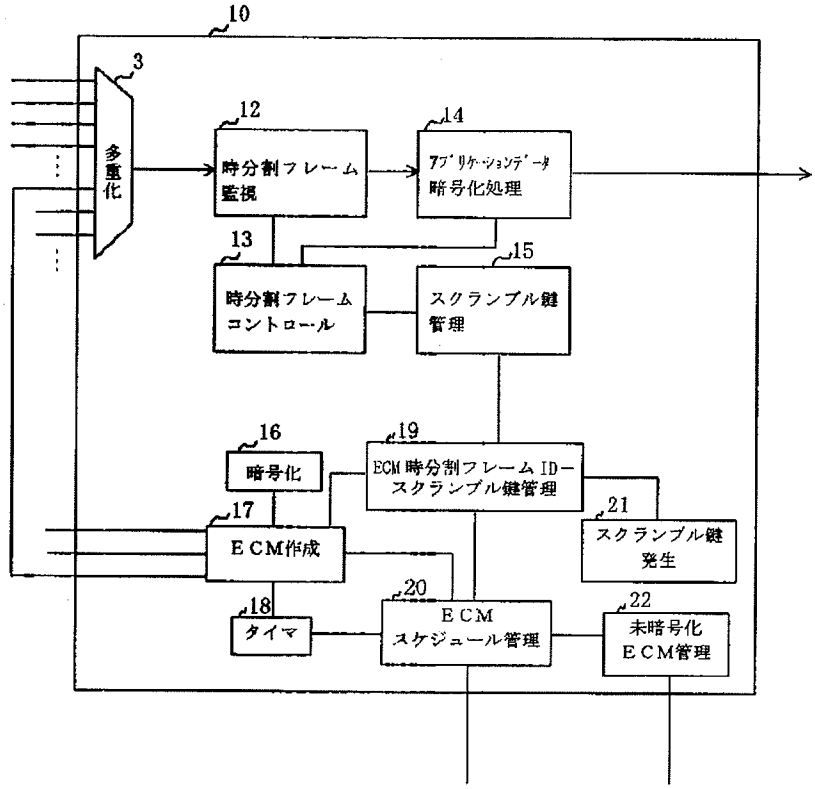
【図17】

図17


ECMﾃﾞｰﾀ
時分割ﾌﾚｰﾑID
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀA1の時分割ﾌﾚｰﾑID
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀA1'の時分割ﾌﾚｰﾑID
ｽｸﾗﾝﾌﾞﾙ鍵
Kn 2
Kn-1
Kn
Kn+1
Kn+2
m
m：ECMﾃﾞｰﾀの
時分割ﾌﾚｰﾑID数

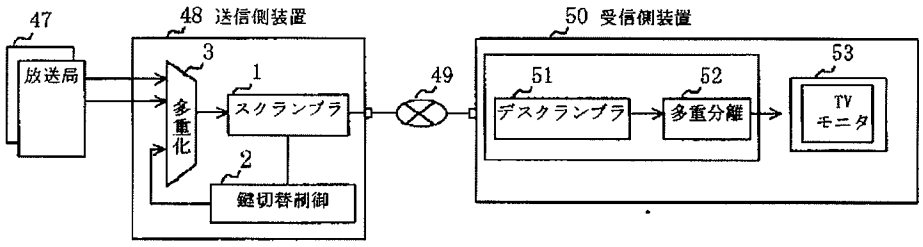
【図8】

図8


10
3
多重化
12
時分割フレーム監視
14
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀ暗号化処理
13
時分割フレームコントロール
15
スクランブル鍵管理
16
暗号化
19
ECM時分割フレームID－スクランブル鍵管理
21
スクランブル鍵発生
17
ＥＣＭ作成
18
タイマ
20
ＥＣＭスケジュール管理
22
未暗号化ＥＣＭ管理

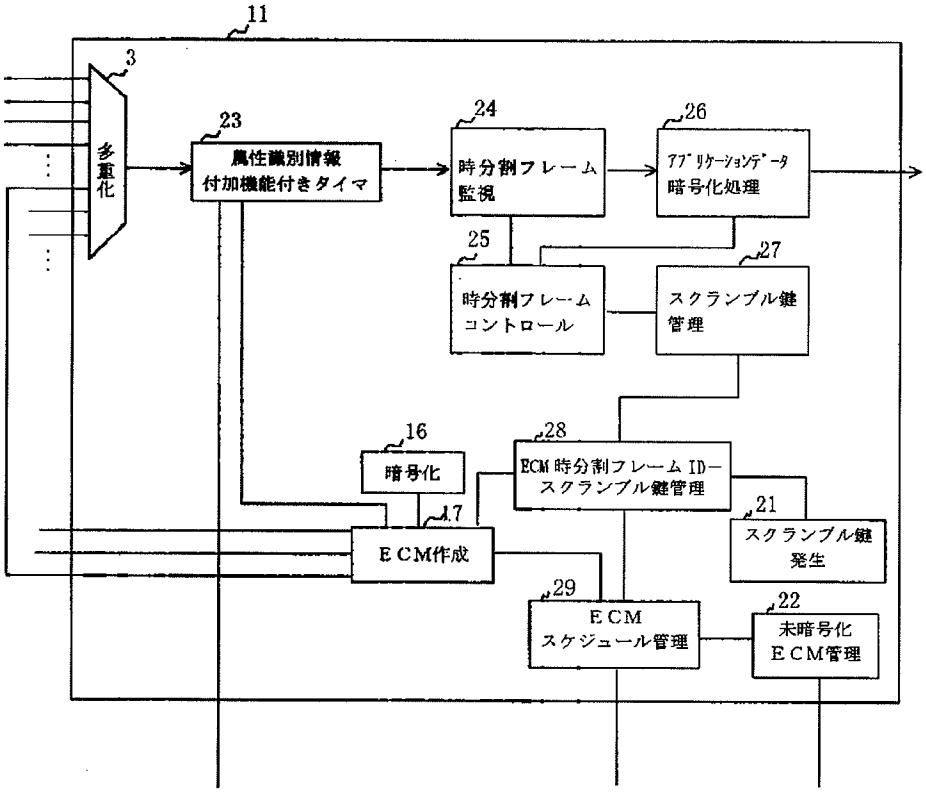
【図18】

図18


47
放送局
48 送信側装置
3
多重化
1
スクランブラ
2
鍵切替制御
49
50 受信側装置
51
デスクランブラ
52
多重分離
53
TV モニタ

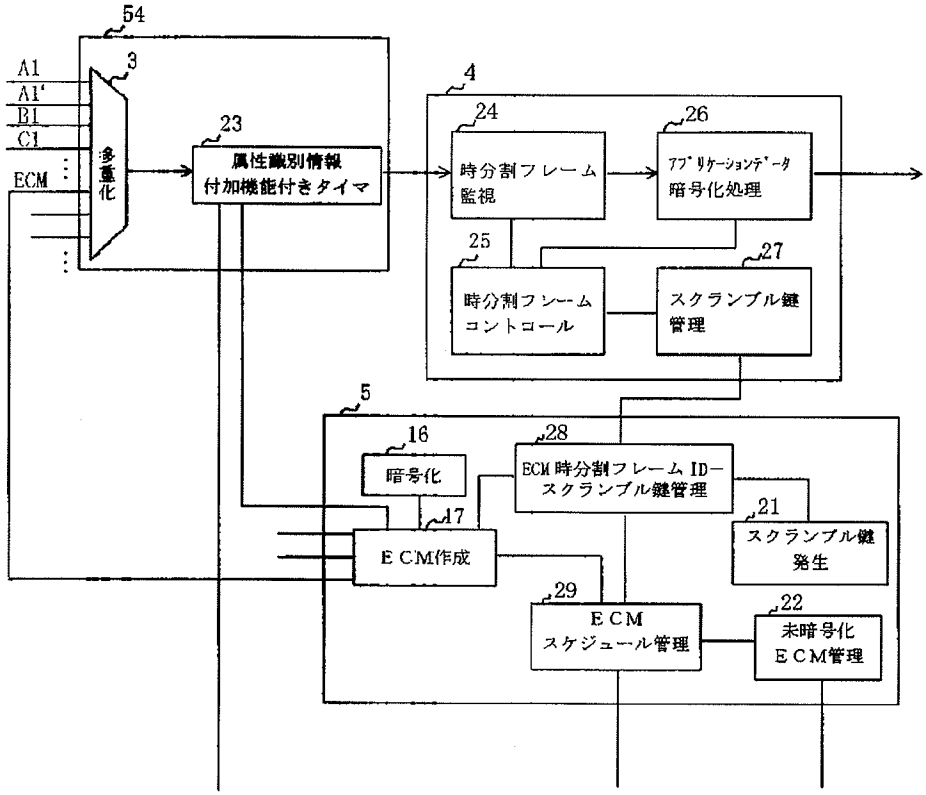
【図9】

図9


11
3
多重化
23
属性識別情報
付加機能付きタイマ
24
時分割フレーム
監視
26
ｱﾌﾟﾘｹｰｼｮﾝﾃﾞｰﾀ
暗号化処理
25
時分割フレーム
コントロール
27
スクランブル鍵
管理
16
暗号化
28
ECM時分割フレームID－
スクランブル鍵管理
21
スクランブル鍵
発生
17
ECM作成
29
ECM
スケジュール管理
22
未暗号化
ECM管理

【図１９】

図１９



フロントページの続き

(51) Int.Cl.6	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　7/167			Ｈ０４Ｎ　7/167	